Extreme Networks®

Extreme Management Center User Guide

Legal Notices

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

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

Trademarks

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

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

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

Contact

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

- Global Technical Assistance Center (GTAC) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.

- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks® Software License Agreement

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

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.

2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.

   - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).

   - *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.

5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

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

7. TITLE AND PROPRIETARY RIGHTS
   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.
   b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.
8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the

confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

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

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

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

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

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

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but

not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

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

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.
Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California,

without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.

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

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

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

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

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

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

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

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

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

Table of Contents

Extreme Management Center Help

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

Contact your sales representative for information on obtaining a Extreme Management Center license.

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

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

Extreme Management Center Features

Extreme Management Center provides the following features:

- Network — Device details for all managed devices in the network with sorting and filtering of relevant information for network troubleshooting and forensics. Additionally, create maps of the devices and wireless APs on your network. Import images of maps and building/floor plans, and then drag and drop your managed devices and wireless APs in the map. Use the Search to find a device, AP, or wired/wireless client or locate end-systems for a single AP on the map using RSS-based location services. If you have a NetSight Advanced License (NMS-ADV), this feature also includes maps with triangulated location.
- Alarms & Events — Alarm and event details for all managed devices in the network with sorting and filtering of relevant information for network troubleshooting and forensics.
- Control — Dashboards, reports, and control capabilities extending network management to the network attached end-systems. Allows better visibility and

control for IT analysts, troubleshooters, and helpdesk based on end-system and user identity. Create policies for users and ports, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

- Analytics — Real-time NetFlow data for enhanced network diagnostics such as flow details, applications, senders, and receivers.
- Wireless — Wireless monitoring providing details, dashboards, and Top N information to monitor the overall status of the wireless network, as well as the ability to drill in to details as needed.
- Governance — Oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.
- Reports — Historical and real-time reporting offering high-level network summary information as well as detailed reports and drill-downs.
- Administration — Extreme Management Center administration tools to monitor and maintain the Extreme Management Center application and its components.
- Connect — Provides configuration to allow you to integrate third-party software with Extreme Management Center's Extreme Access Control solution.
- Search — A powerful diagnostic tool to search end-systems by MAC address, IP address, end-system name, or user name for fast troubleshooting. Includes a Search with Compass option that uses SNMP to provide information about the status, configuration, and activities at the ingress points of your network, and is an easy way to search for end stations or users on end stations.

Document Version

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

Date	Revision Number	Description
3-18	8.1 Revision -00	Extreme Management Center 8.1 release

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

PN: 9035223-02

Getting Started with Extreme Management Center

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

Requirements

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

Extreme Management Center License Requirements

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

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

Extreme Management Center Access Requirements

Access to the Extreme Management Center application and its features is determined by the user's membership in a Extreme Management Center authorization group and the group's assigned capabilities. The following table lists the different Extreme Management Center access options and features, and their corresponding capabilities. For more information on how to configure capabilities and authorization group membership, see the Extreme Management Center Help topic "How to Configure User Access to Extreme Management Center Applications," located in the Extreme Management Center Suite-Wide Tools user guide in the "Authorization Device Access" section.

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

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

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

Here are several scenarios that show how different Extreme Management Center user access levels can be configured based on assigned capabilities.

Use Case 1: Full Read/Write Access

To provide full read/write access to all Extreme Management Center functionality, configure user membership in an authorization group assigned the following capabilities:

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

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

Use Case 2: Read-Only Access

To provide read-only access to all Extreme Management Center reports and FlexViews, configure user membership in an authorization group assigned the following capabilities:

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

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

Use Case 3: Limited Read-Only Access

To provide limited read-only access to only Extreme Management Center reporting and wireless data, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight Console > Wireless Manager > Launch

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

To provide read-only access to Extreme Management Center end-system information, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Identity and Access > OneView End-Systems Read Access

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

To provide read/write access to Extreme Management Center end-system information, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access

Browser Requirements

The following web browsers are supported:

- Microsoft Edge and Internet Explorer version 11
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

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

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

Screen Resolution

For optimum display of graphs and tables, Extreme Management Center is best viewed on a system with a minimum screen resolution of 1280x1024.

Enable Report Data Collection

To view Extreme Management Center reporting data, you must enable statistics collection for your network devices. You must be a member of an authorization group that has been assigned the NetSight OneView > Access NetSight OneView and Administration capability to enable data collection. Data collection is not available with the NMS-BASE license.

Enable Device Statistics Collection

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

- **Historical Mode** — Device and physical port statistics are saved to the database and aggregated over time, and are then used in Extreme Management Center reports. The device statistics are also used for active threshold alarms configured in the

Console Alarms Manager.

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

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

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

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

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

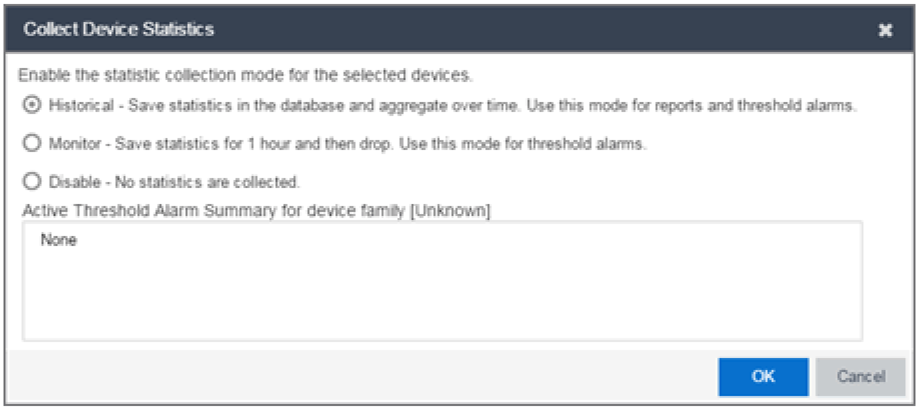
Steps for Enabling Collection

Use the following steps to enable device statistics collection.

1. You can enable statistics collection from either Extreme Management Center or Console:
   - In the **Network** tab, right-click one or more devices (multiple devices must be in the same device family) and select **Device > Collect Device Statistics**. You can also click the **Menu** icon (≡) in the upper left corner of the **Network** tab and select **Device > Collect Device Statistics**.
   - In the Console device tree or **Device Properties** tab, right-click one or more devices (multiple devices must be in the same device family) and select

OneView > Collect Device Statistics.

2. From the Collect Device Statistics window, select the statistic collection mode you want to use: **Historical** or **Monitor**.



Collect Device Statistics

Enable the statistic collection mode for the selected devices.

● Historical - Save statistics in the database and aggregate over time. Use this mode for reports and threshold alarms.

○ Monitor - Save statistics for 1 hour and then drop. Use this mode for threshold alarms.

○ Disable - No statistics are collected.

Active Threshold Alarm Summary for device family [Unknown]

None

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

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

3. Click **OK**. Extreme Management Center begins collecting statistics for the selected devices.

Enable Interface Statistics Collection

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

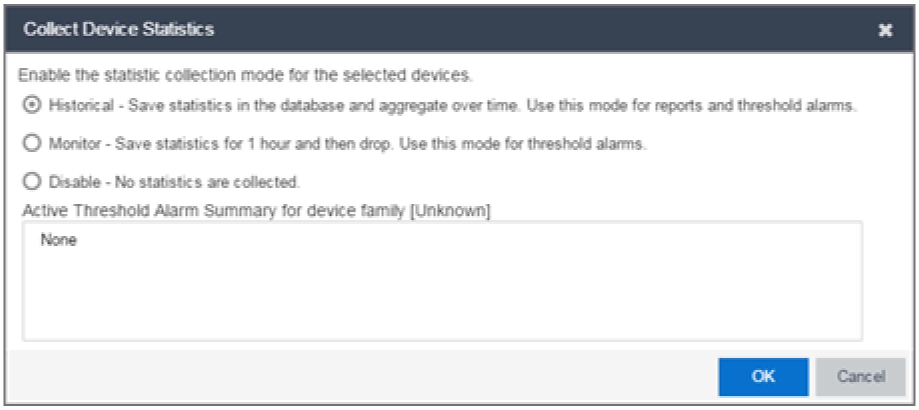
- Historical Mode — Interface statistics are saved to the database and aggregated over time, used in Extreme Management Center reports. The interface statistics are also used for active threshold alarms configured in the **Alarms and Events** tab.
- Monitor Mode — Interface statistics are saved to a Monitor cache for one hour and then dropped. These statistics are used for active threshold alarms configured in the

Console Alarms Manager, but not for Extreme Management Center reporting. (Note that the Monitor mode option is not available if you have disabled Monitor Collection in the OneView Collector Advanced Settings window in the **Administration** > **Options** tab.)

Steps for Enabling Collection

Use the following steps to enable interface statistics collection.

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



Collect Device Statistics

Enable the statistic collection mode for the selected devices.

● Historical - Save statistics in the database and aggregate over time. Use this mode for reports and threshold alarms.

○ Monitor - Save statistics for 1 hour and then drop. Use this mode for threshold alarms.

○ Disable - No statistics are collected.

Active Threshold Alarm Summary for device family [Unknown]

None

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

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

3. Click **OK**. Extreme Management Center begins collecting statistics for the selected interfaces.

Enable Wireless Controller Statistics Collection

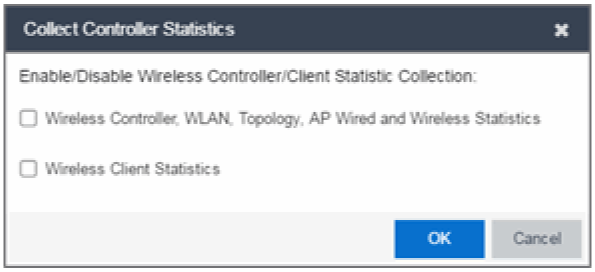
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

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

Steps for Enabling Collection

Use the following steps to enable wireless controller statistics collection.

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



Enable/Disable Wireless Controller/Client Statistic Collection:

□ Wireless Controller, WLAN, Topology, AP Wired and Wireless Statistics

□ Wireless Client Statistics

3. Click **OK**. Extreme Management Center begins collecting statistics for the selected controllers.

Enable Flow Collection

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

Enable Flow Collection on a Device

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

Enable Flow Collection on an Interface

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

Extreme Management Center Scalability

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

Variables		Scenario 1	Scenario 2
Data Retention	Raw Data	7 Days	7 Days
	Hourly Rollups	8 Weeks	8 Weeks
	Daily Rollups	6 Months	6 Months
Polling Interval		15 Minutes	15 Minutes
Devices	Wireless Controllers	5	10
	Wireless APs	1000	2000
	Advanced Switch/Routers	150	50
	Advanced Interfaces	1000	200
	Servers	150	50
Collected Objects		19,450	18,630

Extreme Management Center Timeout

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

Network

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

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

- Console
- MIB Tools

Navigating the Network Tab

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

- Dashboard — Displays summary Extreme Management Center data including switch, network and interface statistics, the five most recent alarms, important wireless data, as well as archive, backup, database, and scheduled event information.
- Devices — Provides you with information about the devices on your network and the relationships between devices. The **Devices** tab also allows you to organize devices into groups, geographically in maps, and configure default settings for newly discovered devices using sites.
- Discovered — Displays newly discovered devices on your network and allows you to configure those devices.
- Firmware — Allows you to view and upgrade firmware for network devices.
- Archives — Displays all device archives, or saved device configurations grouped by device type.
- Reports — Provides a variety of system reports that give information about your devices, ports, and network traffic.

Additionally, the Menu icon (≡) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Dashboard

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

The **Dashboard** contains three options, the Impact Analysis, Overview, Inventory dashboards.

Impact Analysis

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

Overview

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

Inventory

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

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

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

- Asset Tracking — provides a list of devices based on their asset tag. An asset tag is a unique asset number assigned to a device for inventory tracking purposes.
- Device Tracking — allows you to view a history of device attributes and monitor changes made to devices.

Devices

Select the **Devices** tab to display information about devices in your network and the maps and sites in which they are added. The left-panel of the Devices tab contains a drop-down menu, allowing you to view all of your devices, a subset of devices, your maps, or your sites. Selecting a device, device group, map, or site in the Groups/Maps navigation tree displays details about the item you selected in the right-panel.

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

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

Discovered

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

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

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

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

Firmware

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

Archives

Select the Archives tab to create new archives for your devices and view a list of existing archives grouped by device type in the left-hand panel. This tab provides information about archive operations performed on the selected device or device group. Additionally, use your archives to compare your device configurations against industry best practices.

Reports

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

- Device
- Interface
- Network

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

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

Related Information

For information on related topics:

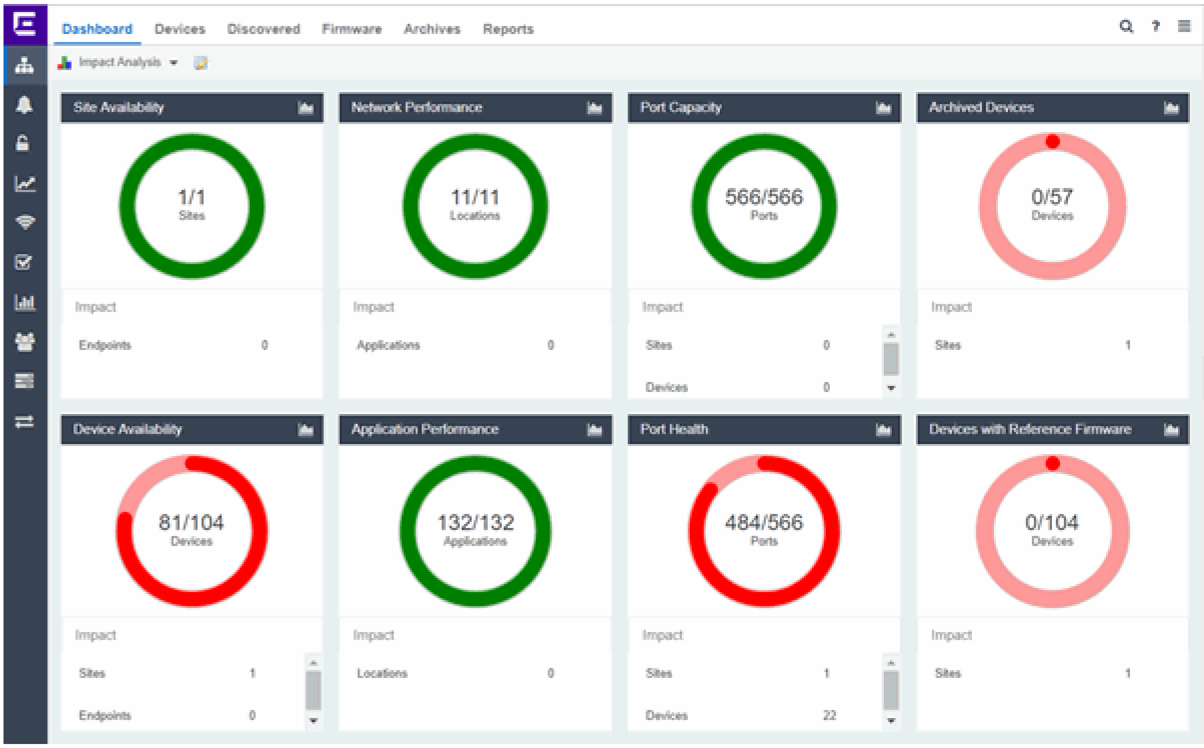
- Device Operations
- Search

For information on related tasks:

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

Impact Analysis Dashboard Overview

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



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

- A network element is considered **"faulting"** if it is non-optimal relative to a certain factor; for example, a device that has not been archived recently or an application that is responding poorly.
- A network element is considered **"impacted"** if it has a relationship to a faulting element which might affect its operation; for example, an endpoint connected to a device that failed.

Charts

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

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

The Impact Status is reflected by color:

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

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

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

Site Availability

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

- Click the ring chart to open the Unavailable Sites report that displays sites Extreme Management Center can not reach.
- Click **Endpoints** in the Impact Summary beneath the ring chart to open the Endpoints Impacted by Unavailable Sites report that provides more details about endpoints with devices.

- Click the report button (📈) to open the Site Availability History report that provides a historical view of the Site Availability chart.

Device Availability

The center of the Device Availability ring chart indicates the ratio of devices with which Extreme Management Center can communicate to the total number of devices. The number of sites and endpoints that contain devices with which Extreme Management Center can not communicate are listed in the Impact Summary beneath the ring chart.

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

Network Performance

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

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

- Click the ring chart to open the Slow Locations report that displays locations with slower-than-expected network response times.
- Click **Applications** in the Impact Summary beneath the ring chart to open the Applications Impacted by Slow Locations report that provides more details

about the tracked applications and network services impacted by slower-than-expected network response time.

NOTE: Enable Event Collection to allow Extreme Management Center to report specific end-points impacted by slower-than-expected response times.

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

Application Performance

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

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

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

NOTE: Enable Event Collection to allow Extreme Management Center to report specific end-points impacted by slower-than-expected response times.

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

Port Capacity

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

- Click the ring chart to open the Highly Utilized Ports report that displays the utilization of ports filtered to include only those ports with an excessive port rate.
- Click **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Highly Utilized Ports report that provides more details about sites impacted by port capacity.
- Click **Devices** in the Impact Summary beneath the ring chart to open the Devices Impacted by Highly Utilized Ports report that provides more details about devices impacted by port capacity.
- Click the report button (📈) to open the Port Capacity History report that provides a historical view of the Port Capacity chart.

Port Health

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

- Click the ring chart to open the High Error Ports report that lists the ports with an excessive error rate.
- Click **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by High Error Ports report that provides a list of sites with ports with an unacceptable error rate.

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

Archived Devices

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

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

Devices with Reference Firmware

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

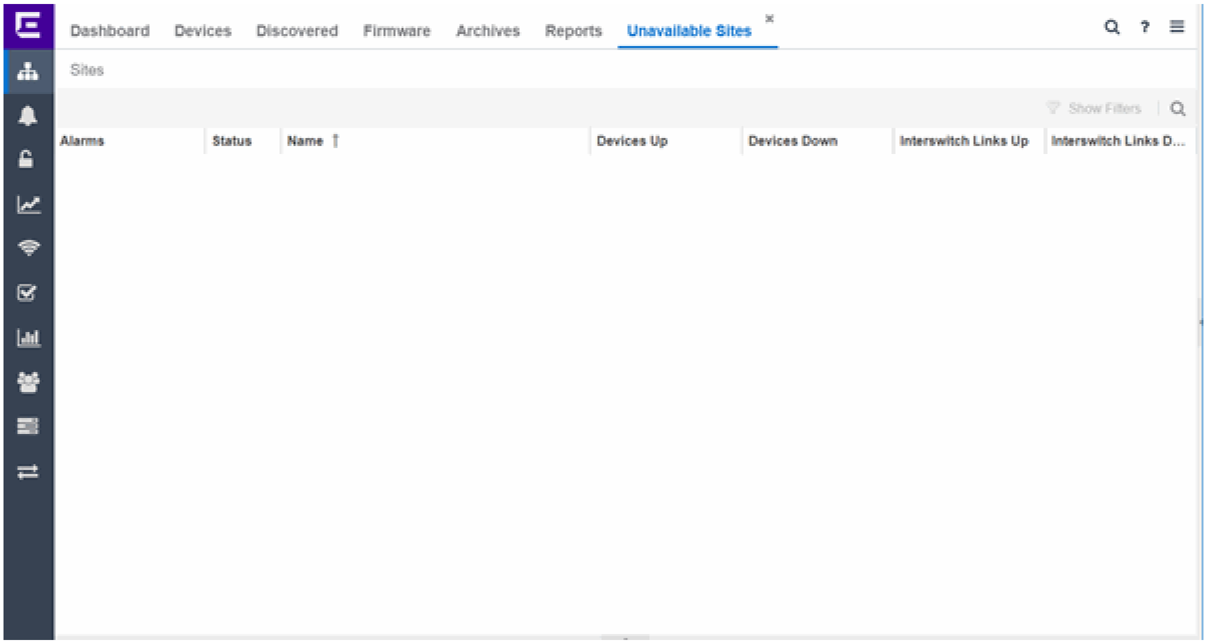
- Click the ring chart to open the Devices Without Reference Firmware report that displays a list of affected devices not running reference firmware.
- Click **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Devices Without Reference Firmware report that provides a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

Related Information

- Impact Analysis Options
- Extreme Management Center Network Tab Overview

Unavailable Sites Report

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



Alarms	Status	Name ↑	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links D...

The following columns are included in the report:

Alarms:

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

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

Status:

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

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

Name:

The name of the site.

Devices Up

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

Devices Down

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

Interswitch Links Up

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

Interswitch Links Down

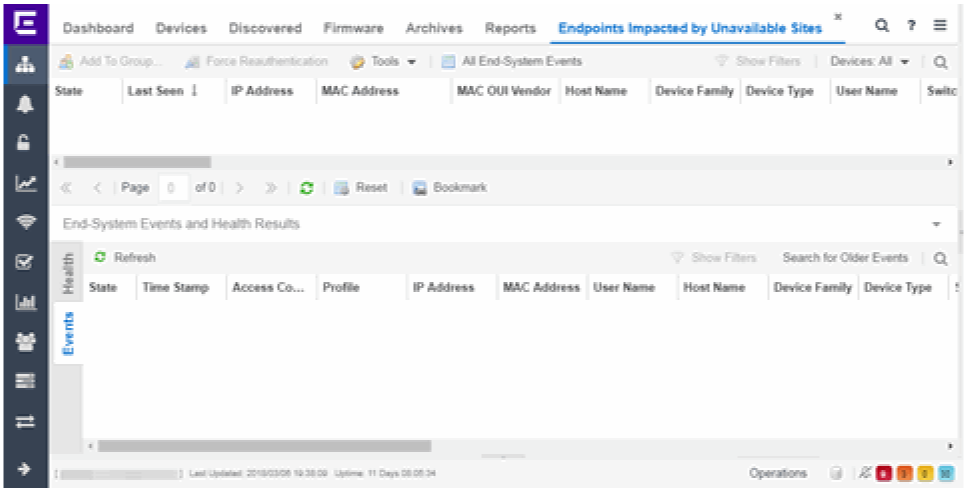
This column indicates the number of Interswitch Links with a Status of Down in the site.

Related Information

- Impact Analysis Dashboard Overview

Endpoints Impacted by Unavailable Sites Report

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



The report contains three tables:

- End-System Information
- Events
- Health

End-System Information

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

ID

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

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.

- Error - Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Extreme Management Center
  - the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Access Control) are incorrect for the assessment server

Last Seen

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

IP Address

The end-system's IP address.

OV MAC Key

OV MAC Key. This column is hidden by default.

MAC Address

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

MAC OUI Vendor

The vendor associated with the MAC OUI.

Host Name

The end-system's host name.

Device Family

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

Device Type

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

User Name

The User Name used for device access.

Switch IP

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

Switch Nickname

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

Switch Port

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

Policy

The policy role assigned to the end-system.

Authorization

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

Risk Level

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

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

Profile Name

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

Reason

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

Authentication Type

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

State Description

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

Extended State

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

Access Control Engine/Source IP

The Engine to which the end-system is connecting.

Engine Group

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

RFC 3580 VLAN ID

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

Warning Time

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

Last Quarantined

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

Score

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

Top Score

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

Actual

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

Switch Port Index

The switch port index to which the end-system connected.

Switch Location

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

ELIN

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

Port Info Raw

Displays unformatted information as it is received from the port.

All Authentication Types

This column displays all the authentication methods the end-system has used to authenticate.

Last Scan Result State

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

Last Scanned Time

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

First Seen Time

he first time the end-system was seen by the NAC appliance.

NAP Capable

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

Custom 1-4

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

Registered User

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

Registered Email

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

Registered Phone

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

Sponsor

The registered device's sponsor.

Registration 1-5

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

Registration Description

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

Groups

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

Group 1-3

Displays the names of up to three end-system groups.

Zone

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

Request Attributes

Indicates if attributes have been requested

Registration Type

Shows the type of registration

RADIUS Server IP

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

Source

Displays the origin of the event:

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

DCM

Data Center Manager. This column is hidden by default.

TLS Client Certificate Expiration

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

TLS Client Certificate Issuer

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

Events Log

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

ID

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

State

The end-system's connection state:

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

- the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Assessment Server) are incorrect for the assessment server

Timestamp
Shows the date and time when an event occurred.

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

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

IP Address
The end-system's IP address.

MAC Address
The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected in the Display section of the Access Control Options (Administration > Options > Access Control).

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

Host Name
The end-system's host name.

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

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

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

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

Reason

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

Authorization

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

Auth Type

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

Switch IP

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

Switch Nickname

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

Switch Port Index

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

Switch Port

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

Switch Location

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

ELIN

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

Port Info Raw

Displays unformatted information as it is received from the port.

Last Scan Time

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

Zone

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

Registration Type

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

RADIUS Server IP

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

Event Source

Displays the origin of the event:

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

Health Log

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

Risk

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

Name

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

Test Case ID

The unique number assigned to the test case.

Score

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

Scoring Mode

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

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

CVE IDs

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

Description

This column lists information about the health result detail.

Solution

This column lists a solution for the health result.

Port ID

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

Protocol ID

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

Assessment

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

Remediation

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

Type

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

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

Related Information

- Impact Analysis Dashboard Overview

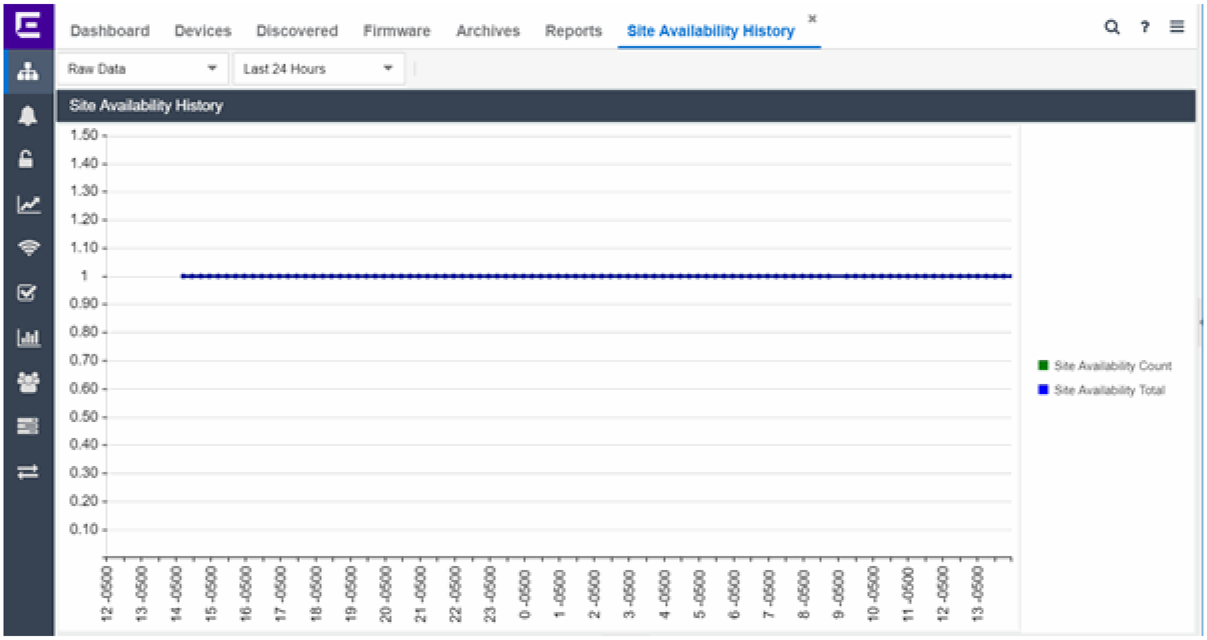
Site Availability History Report

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

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

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

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

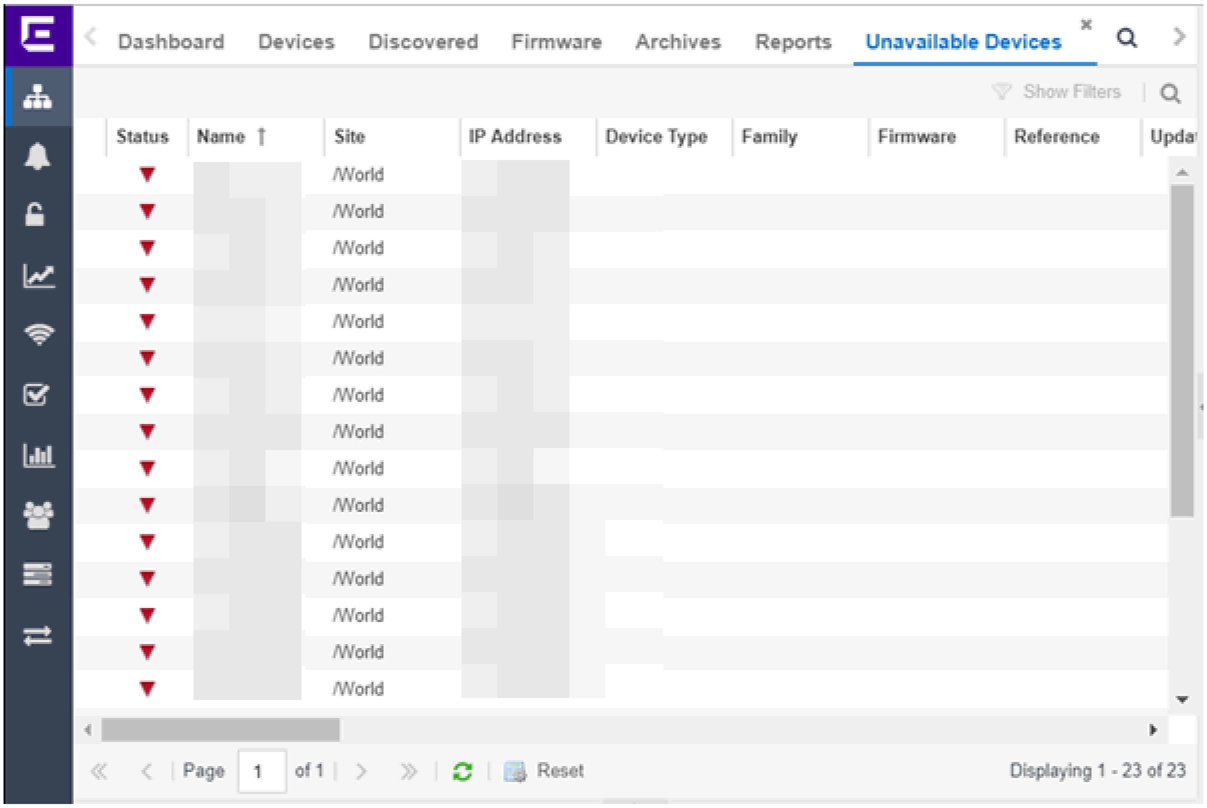


Related Information

- [Impact Analysis Dashboard Overview]

Unavailable Devices Report

The Unavailable Devices report provides detailed information for devices with which Extreme Management Center cannot communicate (Status of **Down**).



Status	Name	Site	IP Address	Device Type	Family	Firmware	Reference	Upda
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					
▼	[redacted]	/World	[redacted]					

Displaying 1 - 23 of 23

The following columns are included in the report:

Device Status

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

- Green icon (●) — Indicates Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center can not contact the device.

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

Status

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

- Red icon (🔻) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.
- Yellow icon (▲) — A warning that might lead to a problem.
- Blue icon (🟦) — Information only; not a problem.
- Green icon (🟢) — Extreme Management Center can contact the device.

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

Device ID

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

Name

The device name, nickname, or IP address.

Site

The site in which the device is located.

Poll Type

This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name

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

Admin Profile

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

Client Profile

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

IP Address

The device's IP address.

Context

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

IP Context

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

Trap Status

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

Syslog Status

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

Display Name

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

Device Type

The type of device.

Family

The device product family.

Firmware

The revision for the firmware running in the device.

Running Reference Firmware

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

Updates

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

Archived

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

Config Changed

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

Policy Domain

The policy domain assigned to the device.

Boot PROM

The revision for the BootPROM installed on the device.

Base MAC

The base MAC address for the device.

Serial Number

The serial number for the device.

Stats

Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.

Location

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

Contact

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

System Name

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

Uptime

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

Nickname

The user-defined nickname for the selected device.

Description

A description of the unavailable device.

User Data 1-4, Notes

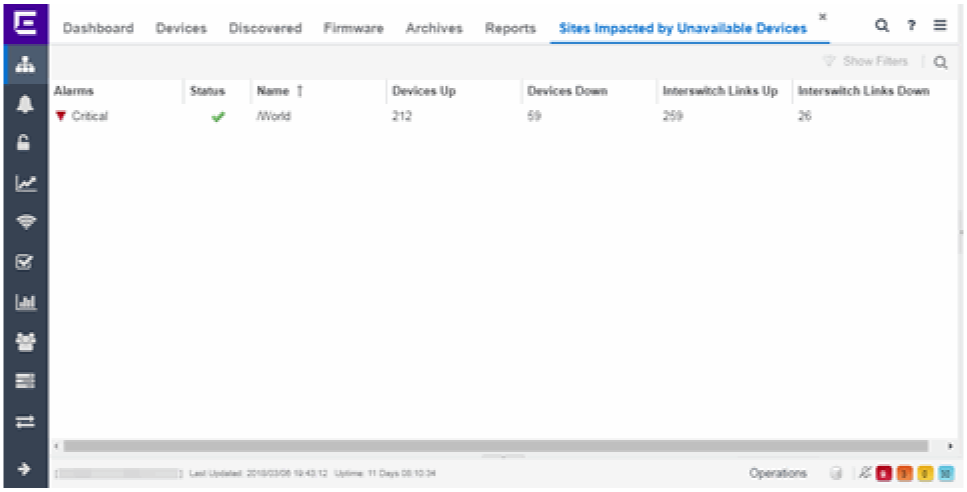
These columns can provide additional information about the device.

Related Information

- Impact Analysis Dashboard Overview

Sites Impacted by Unavailable Devices Report

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



Alarms	Status	Name ↑	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links Down
▼ Critical	✓	/World	212	59	259	26

The following columns are included in the report:

Alarms

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

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

Status

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

down.

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

Name
The name of the site.

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

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

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

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

Related Information

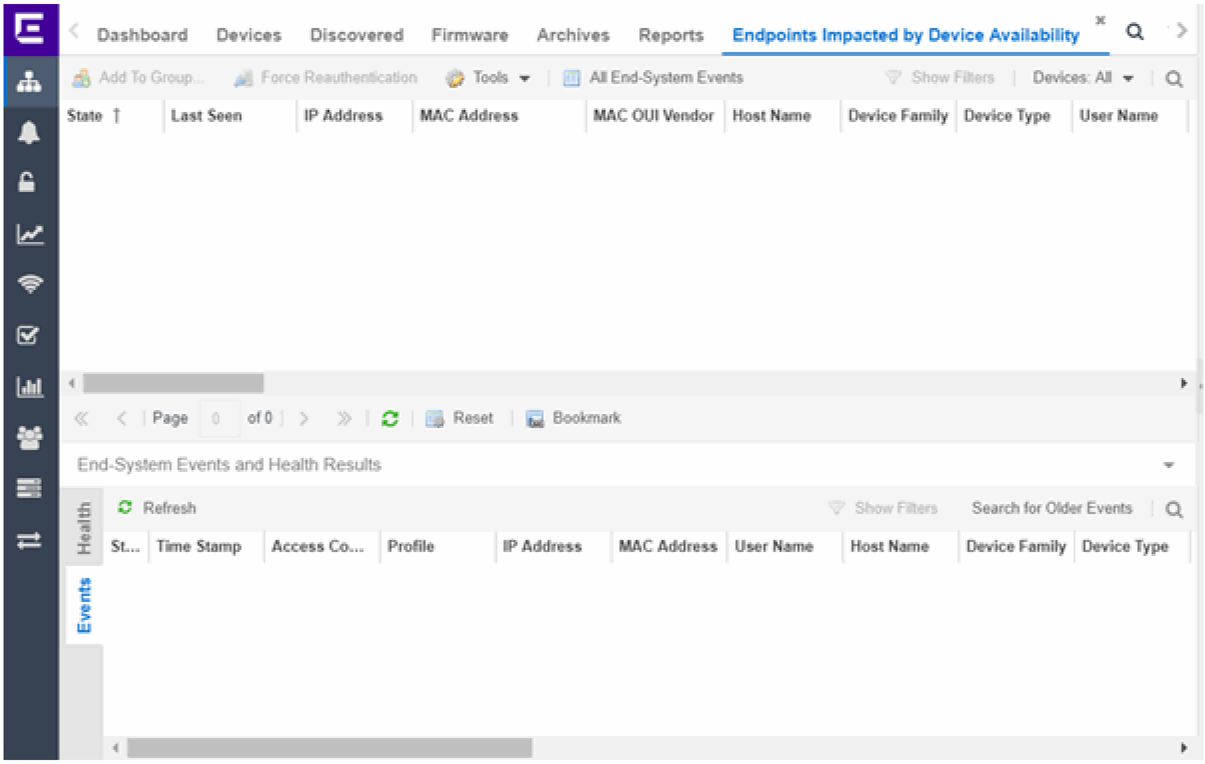
- Impact Analysis Dashboard Overview

Endpoints Impacted by Unavailable Devices Report

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

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

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



State	Last Seen	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name

St...	Time Stamp	Access Co...	Profile	IP Address	MAC Address	User Name	Host Name	Device Family	Device Type

The report contains three tables:

- End-System Information
- Events
- Health

End-System Information

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

ID

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

State

The end-system's connection state:

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

Last Seen

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

IP Address

The end-system's IP address.

OV MAC Key

OV MAC Key. This column is hidden by default.

MAC Address

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

MAC OUI Vendor

The vendor associated with the MAC OUI.

Host Name

The end-system's host name.

Device Family

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

Device Type

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

User Name

The User Name used for device access.

Switch IP

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

Switch Nickname

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

Switch Port

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

Policy

The policy role assigned to the end-system.

Authorization

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

Risk Level

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

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

Profile Name

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

Reason

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

Authentication Type

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

State Description

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

Extended State

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

Access Control Engine/Source IP

The Engine to which the end-system is connecting.

Engine Group

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

RFC 3580 VLAN ID

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

Warning Time

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

Last Quarantined

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

Score

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

Top Score

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

Actual

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

Switch Port Index

The switch port index to which the end-system connected.

Switch Location

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

ELIN

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

Port Info Raw

Displays unformatted information as it is received from the port.

All Authentication Types

This column displays all the authentication methods the end-system has used to authenticate.

Last Scan Result State

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

Last Scanned Time

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

First Seen Time

he first time the end-system was seen by the NAC appliance.

NAP Capable

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

Custom 1-4

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

Registered User

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

Registered Email

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

Registered Phone

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

Sponsor

The registered device's sponsor.

Registration 1-5

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

Registration Description

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

Groups

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

Group 1-3

Displays the names of up to three end-system groups.

Zone

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

Request Attributes

Indicates if attributes have been requested

Registration Type

Shows the type of registration

RADIUS Server IP

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

Source

Displays the origin of the event:

- Access Controlengine — An Access Controlengine.
- Wireless Manager — An ExtremeWireless Controller or AP.

  - ExtremeXOS ID Manager — An Extreme switch running ExtremeXOS with the Identify Manager feature configured to send events to NetSight.
  - OneFabric Connect — An ExtremeConnect module (e.g. Solutions Architecture and Innovation (SAI) integration)
  - One Controller — The Extreme SDN Controller.

DCM

Data Center Manager. This column is hidden by default.

TLS Client Certificate Expiration

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

TLS Client Certificate Issuer

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

Events Log

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

ID

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

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned NAC profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Error - Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant

- all assessment servers are unavailable
- the assessment server can't reach the end-system
- no assessment servers are configured
- the assessment server is not compatible with the current version of NAC Manager
- the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Assessment Server) are incorrect for the assessment server

Timestamp

Shows the date and time when an event occurred.

Access Control engine / Source IP

The NAC appliance to which the end-system is connecting.

Profile

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

IP Address

The end-system's IP address.

MAC Address

The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected in the Display section of the Access Control Options (Administration > Options > Access Control).

User Name

The name of the user that triggered the event.

Host Name

The end-system's host name.

Device Family

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

Device Type

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

State Description

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

Extended State

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

Reason

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

Authorization

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

Auth Type

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

Switch IP

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

Switch Nickname

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

Switch Port Index

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

Switch Port

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

Switch Location

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

ELIN

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

Port Info Raw

Displays unformatted information as it is received from the port.

Last Scan Time

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

Zone

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

Registration Type

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

RADIUS Server IP

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

Event Source

Displays the origin of the event:

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

Health Log

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

Risk

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

Name

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

Test Case ID

The unique number assigned to the test case.

Score

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

Scoring Mode

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

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

CVE IDs

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

Description

This column lists information about the health result detail.

Solution

This column lists a solution for the health result.

Port ID

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

Protocol ID

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

Assessment

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

Remediation

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

Type

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

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

Related Information

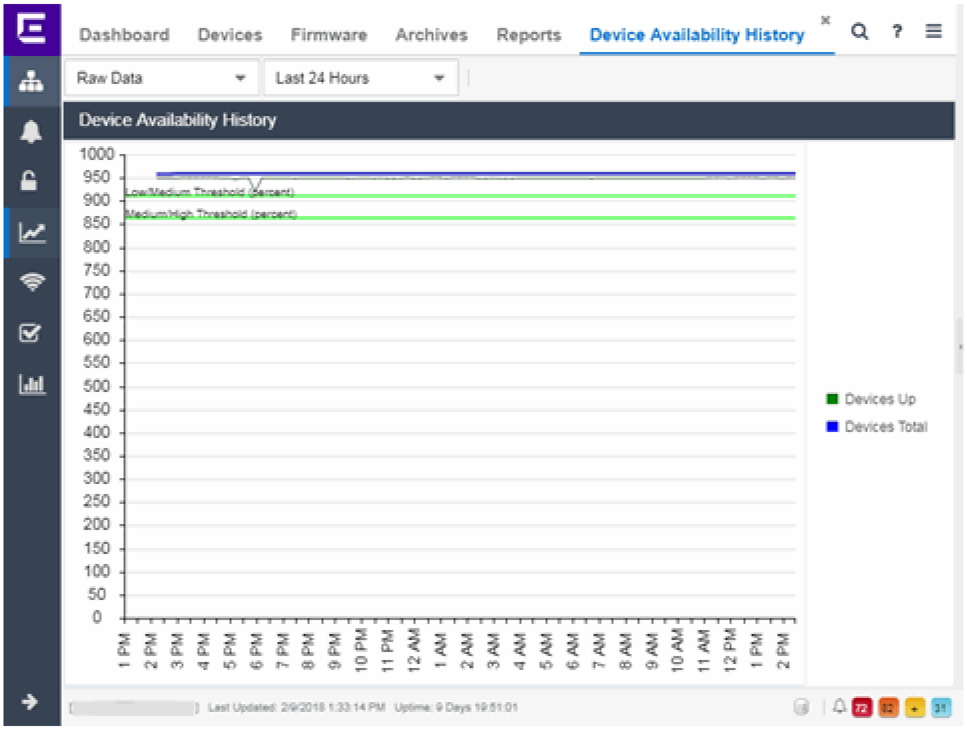
- Impact Analysis Dashboard Overview

Device Availability History Report

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

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

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



Related Information

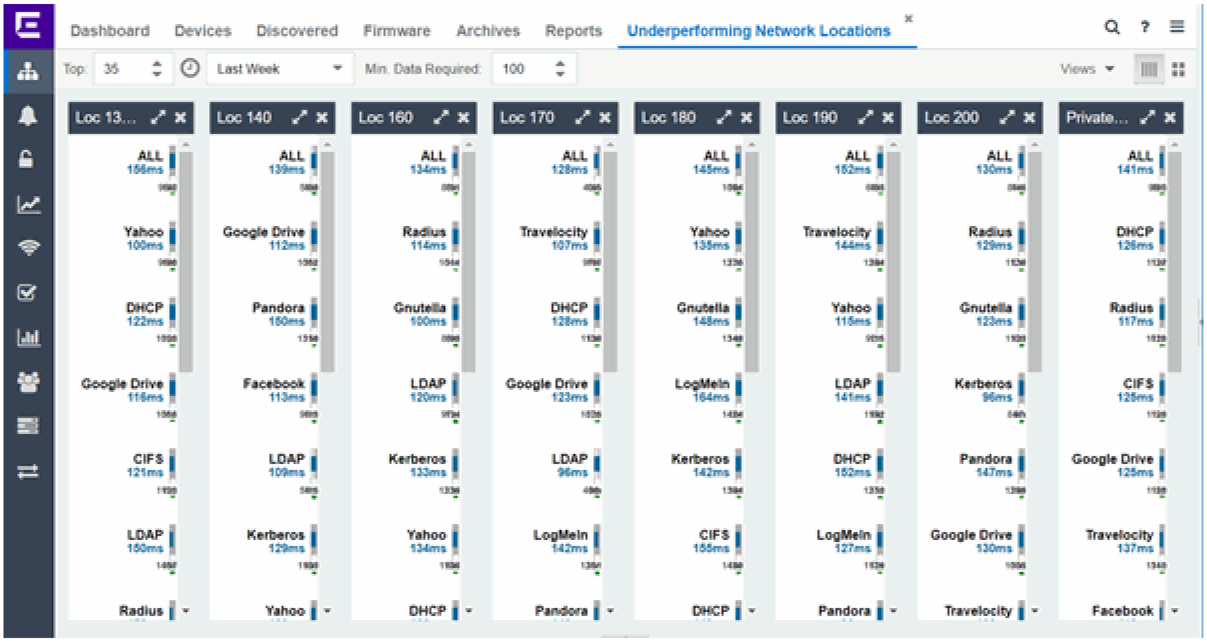
- Impact Analysis Dashboard Overview

Slow Locations Report

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

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

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



Top: 35 Last Week Min. Data Required: 100

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

Top:

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

Time Span

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

Min Data Required

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

Display Format

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

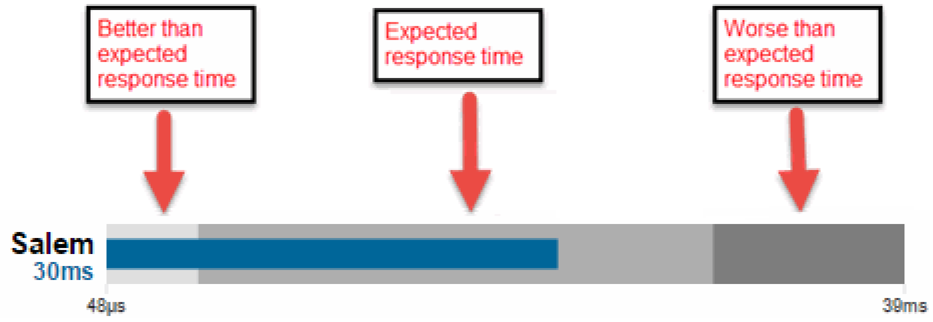
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

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

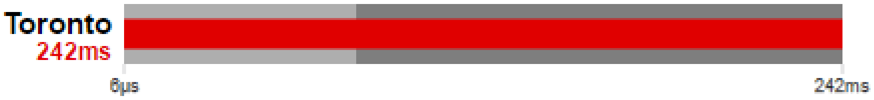
NOTE: The values in this graph are an average of all response times observed every minute.



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

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

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



Historical Response Time

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

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

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

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

Related Information

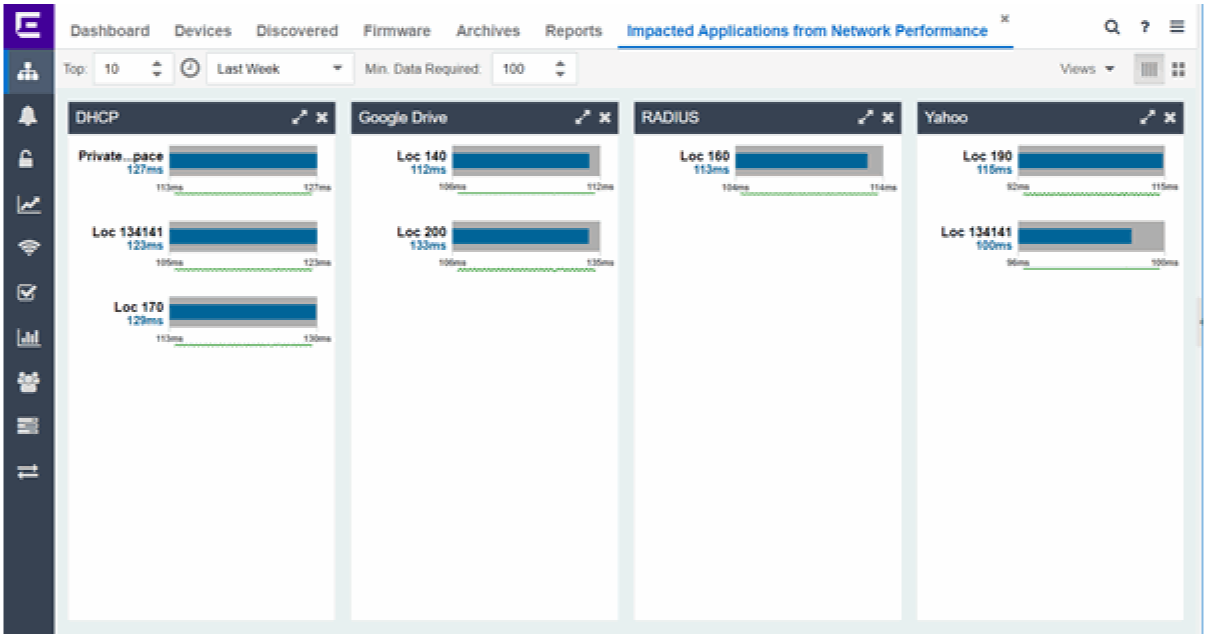
- Impact Analysis Dashboard Overview

Applications Impacted by Slow Locations Report

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

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

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



Top: 10 Last Week Min. Data Required: 100

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

Top

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

Time Span

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

Min Data Required

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

Display Format

Select how data is displayed: Click (||||) to display the data in columns or (▦) to display the data in rows.

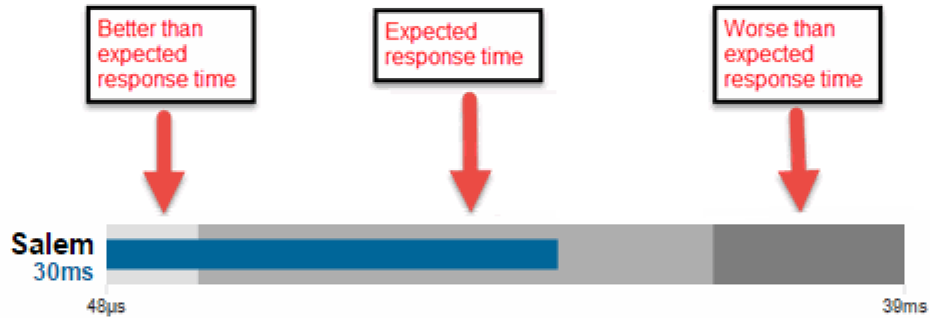
The report contains two graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

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

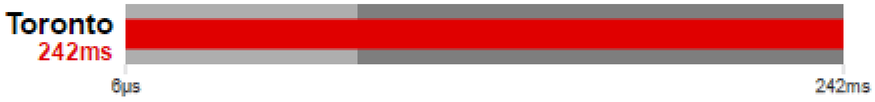
NOTE: The values in this graph are an average of all network response times observed every minute.



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

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

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



Historical Response Time

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

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

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

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

Related Information

- Impact Analysis Dashboard Overview

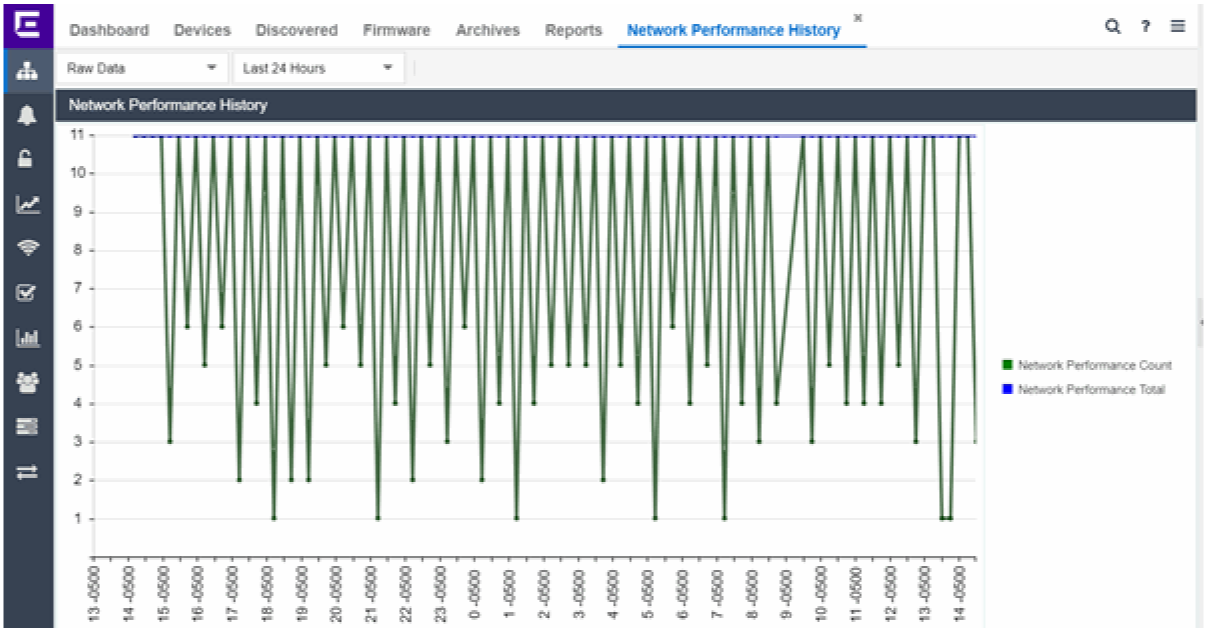
Network Performance History Report

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

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

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

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

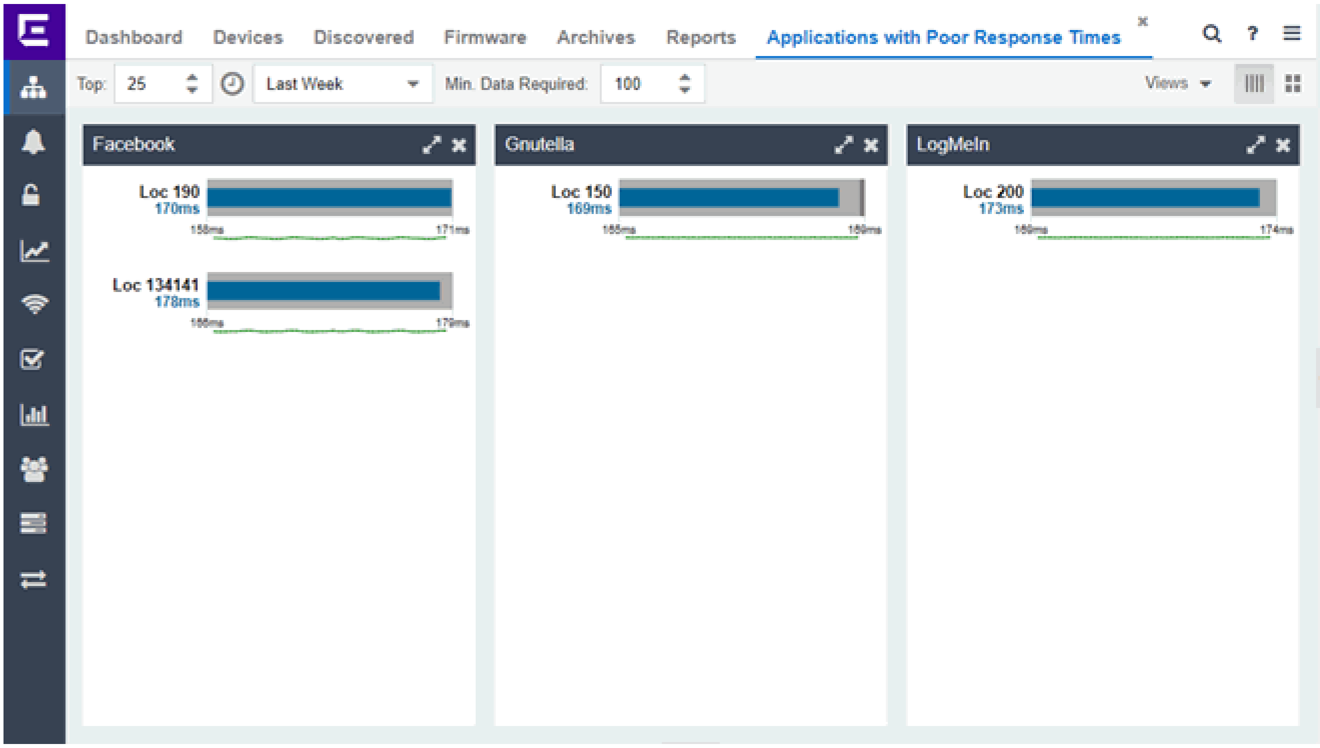


Related Information

- Impact Analysis Dashboard Overview

Slow Applications Report

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



Top: 25

Last Week

Min. Data Required: 100

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

Top:

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

Time Span

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

Min Data Required

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

Display Format

Select how data is displayed: Click (||||) to display the data in columns or (⊞) to display the data in rows.

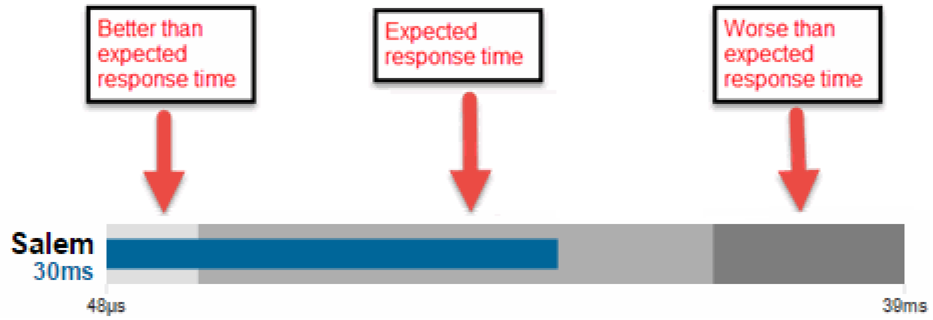
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

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

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


Better than expected response time

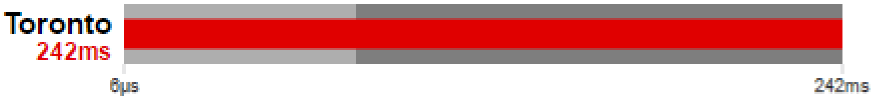
Expected response time

Worse than expected response time

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

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

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



Historical Response Time

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

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

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

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

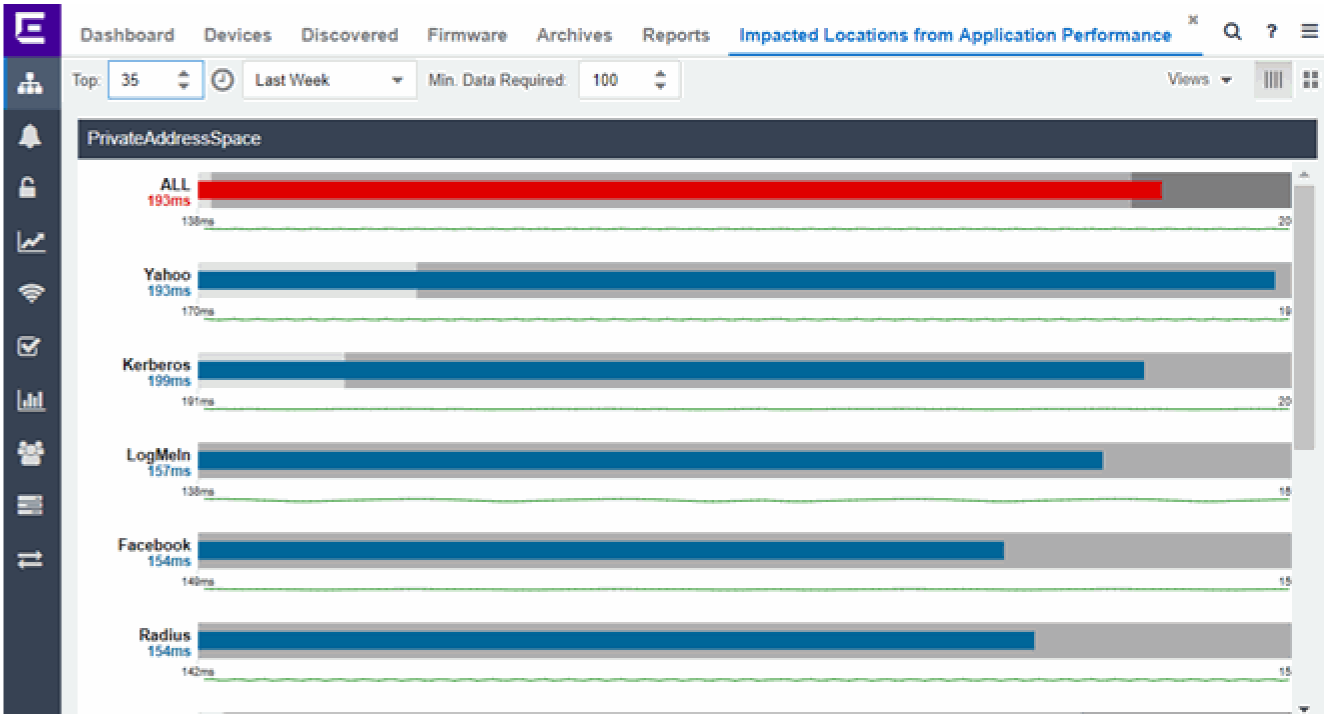
Related Information

- Impact Analysis Dashboard Overview

Locations Impacted by Slow Applications

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

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



Top: 35

Last Week

Min. Data Required: 100

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

Top

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

Time Span

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

Min Data Required

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

Display Format

Select how data is displayed: Click (▥) to display the data in columns or (⊞) to display the data in rows.

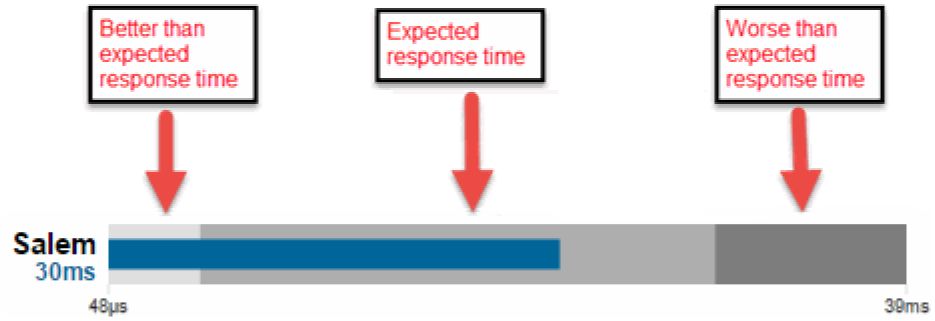
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

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

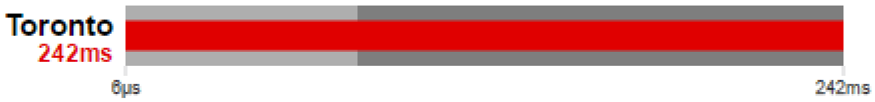
NOTE: The values in this graph are an average of all response times observed every minute.


Better than expected response time
Expected response time
Worse than expected response time
Salem
30ms
48µs
39ms

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

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

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



Historical Response Time

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

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

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

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

Related Information

- Impact Analysis Dashboard Overview

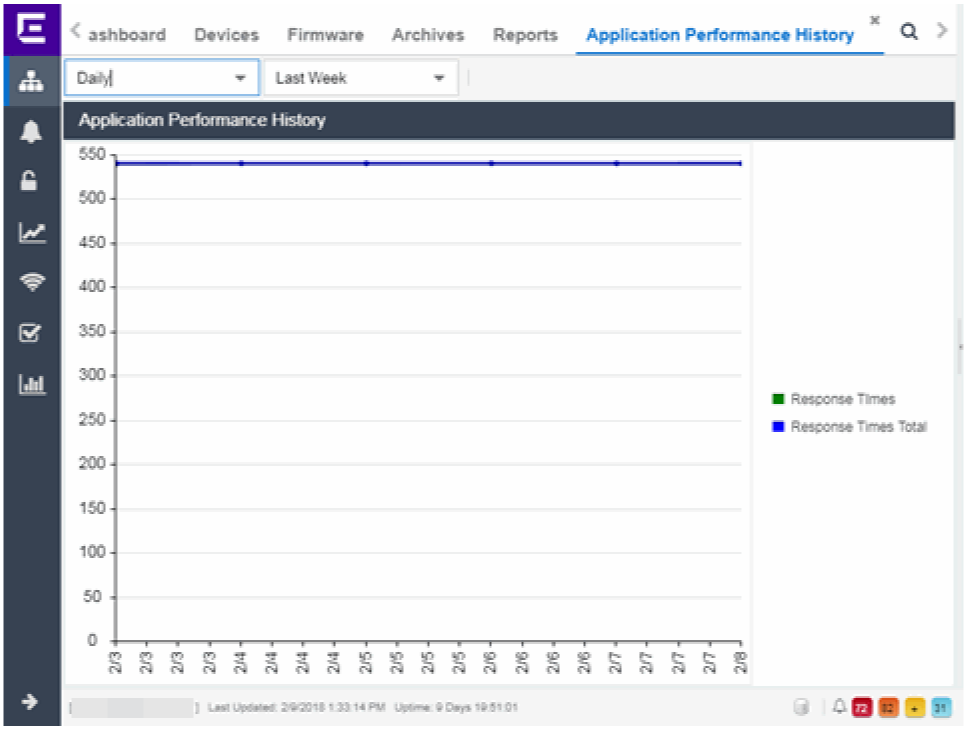
Application Performance History Report

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

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

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

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



Last Updated: 2/9/2018 1:33:14 PM Uptime: 9 Days 19:51:01

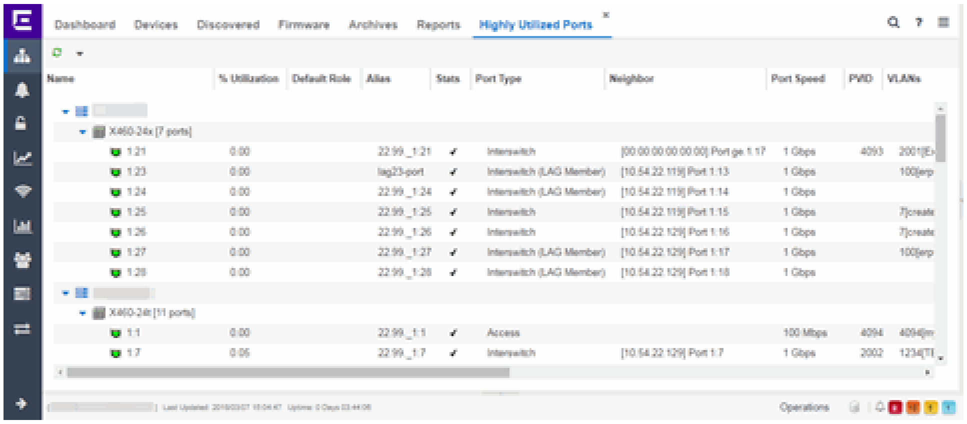
Related Information

- Impact Analysis Dashboard Overview

Highly Utilized Ports Report

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

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port utilization.



Name	% Utilization	Default Role	Alias	Stats	Port Type	Neighbor	Port Speed	PVID	VLANs
[redacted]									
X460-24x [7 ports]									
1:21	0.00		22.99_1:21	✓	Interswitch	[00:00:00:00:00:00] Port ge.1.17	1 Gbps	4093	2001[E
1:23	0.00		lag23-port	✓	Interswitch (LAG Member)	[10.54.22.119] Port 1:13	1 Gbps		100[erp
1:24	0.00		22.99_1:24	✓	Interswitch (LAG Member)	[10.54.22.119] Port 1:14	1 Gbps		
1:25	0.00		22.99_1:25	✓	Interswitch	[10.54.22.119] Port 1:15	1 Gbps		7[create
1:26	0.00		22.99_1:26	✓	Interswitch	[10.54.22.129] Port 1:16	1 Gbps		7[create
1:27	0.00		22.99_1:27	✓	Interswitch (LAG Member)	[10.54.22.129] Port 1:17	1 Gbps		100[erp
1:28	0.00		22.99_1:28	✓	Interswitch (LAG Member)	[10.54.22.129] Port 1:18	1 Gbps		
[redacted]									
X460-24t [11 ports]									
1:1	0.00		22.99_1:1	✓	Access		100 Mbps	4094	4094[m
1:7	0.05		22.99_1:7	✓	Interswitch	[10.54.22.129] Port 1:7	1 Gbps	2002	1234[T

[redacted] | Last Updated: 2018/03/07 15:04:47 Uptime: 0 Days 03:44:06

The following columns are included in the report:

Name
The interface name for the port.

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

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

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

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

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

Neighbor
The port to which the port is connected.

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

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

VLANs

The VLANs to which the port is associated.

Description

A description of the port and the device.

Port Type Details

Additional information about the type of port.

Serial Number

The serial number of the device.

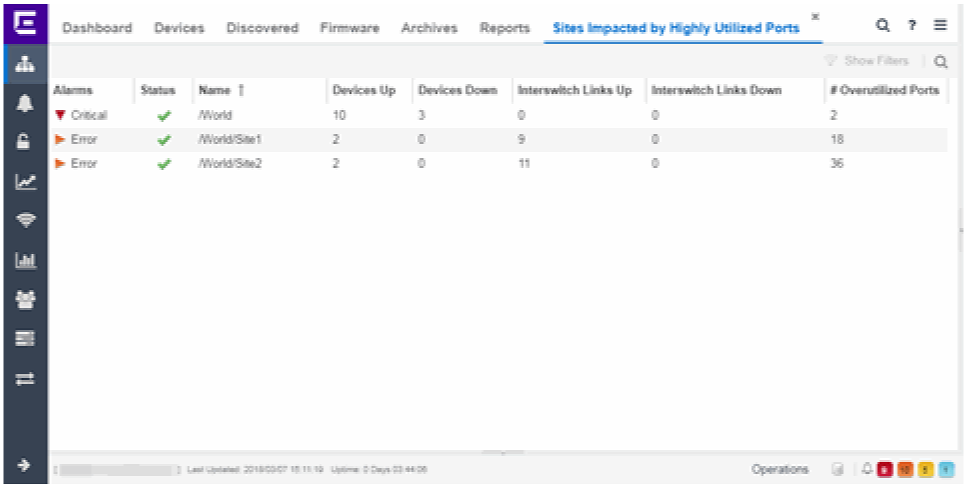
Related Information

- Impact Analysis Dashboard Overview

Sites Impacted by Highly Utilized Ports Report

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

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port utilization.



Alarms	Status	Name	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links Down	# Overutilized Ports
Critical	✓	/World	10	3	0	0	2
Error	✓	/World/Site1	2	0	9	0	18
Error	✓	/World/Site2	2	0	11	0	36

Last Updated: 2018/03/07 15:11:19 Uptime: 0 Days 03:44:06

The following columns are included in the report:

Alarms

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

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

Status

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

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

Name

The name of the site.

Devices Up

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

Devices Down

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

Interswitch Links Up

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

Interswitch Links Down

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

# Overutilized Rate

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

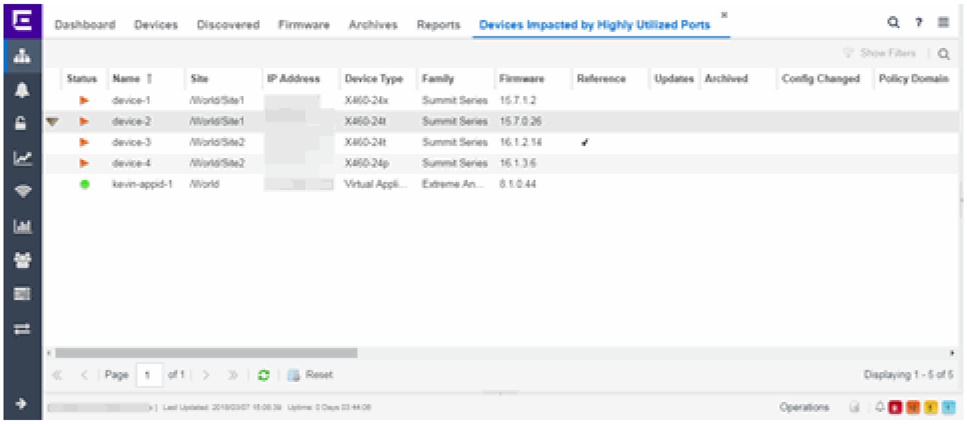
Related Information

- Impact Analysis Dashboard Overview

Devices Impacted by Highly Utilized Ports Report

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

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port utilization.



Status	Name	Site	IP Address	Device Type	Family	Firmware	Reference	Updates	Archived	Config Changed	Policy Domain
▶	device-1	/World/Site1	[redacted]	X460-24x	Summit Series	15.7.1.2					
▶	device-2	/World/Site1	[redacted]	X460-24t	Summit Series	15.7.0.26					
▶	device-3	/World/Site2	[redacted]	X460-24t	Summit Series	16.1.2.14	✓				
▶	device-4	/World/Site2	[redacted]	X460-24p	Summit Series	16.1.3.6					
●	kevin-appid-1	/World	[redacted]	Virtual Appli...	Extreme An...	8.1.0.44					

The following columns are included in the report:

Device Status

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

- Green icon (●) — Indicates Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center can not contact the device.

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

Status

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

- Red icon (▼) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.
- Yellow icon (▲) — A warning that might lead to a problem.
- Blue icon (🟦) — Information only; not a problem.
- Green icon (🟢) — Extreme Management Center can contact the device.

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

Device ID

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

Name

The device name, nickname, or IP address.

Site

The site in which the device is located.

Poll Type

This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name

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

Admin Profile

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

Client Profile

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

IP Address

The device's IP address.

Context

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

IP Context

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

Trap Status

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

Syslog Status

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

Display Name

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

Device Type

The type of device.

Family

The device product family.

Firmware

The revision for the firmware running in the device.

Running Reference Firmware

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

Updates

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

Archived

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

Config Changed

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

Policy Domain

The policy domain assigned to the device.

Boot PROM

The revision for the BootPROM installed on the device.

Base MAC

The base MAC address for the device.

Serial Number

The serial number for the device.

Stats

Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.

Location

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

Contact

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

System Name

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

Uptime

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

Nickname

The user-defined nickname for the selected device.

Description

A description of the unavailable device.

User Data 1-4, Notes

These columns can provide additional information about the device.

Asset Tag

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

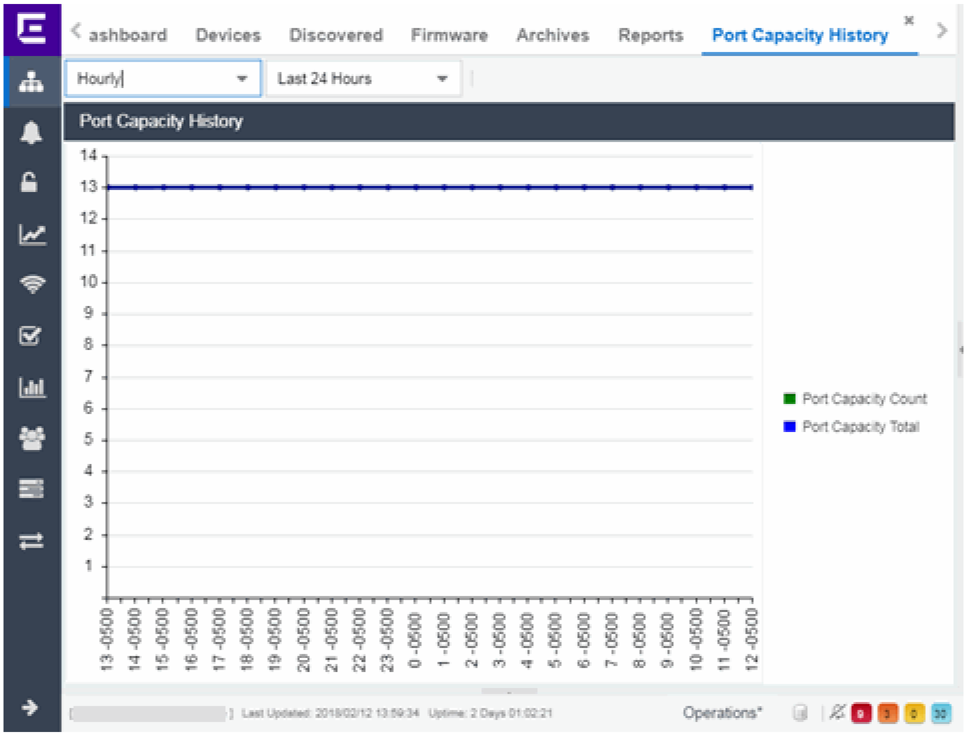
Related Information

- Impact Analysis Dashboard Overview

Port Capacity History Report

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

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port utilization.



Hourly

Last 24 Hours

Last Updated: 2018/02/12 13:59:34 Uptime: 2 Days 01:02:21

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

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

{img placeholder}

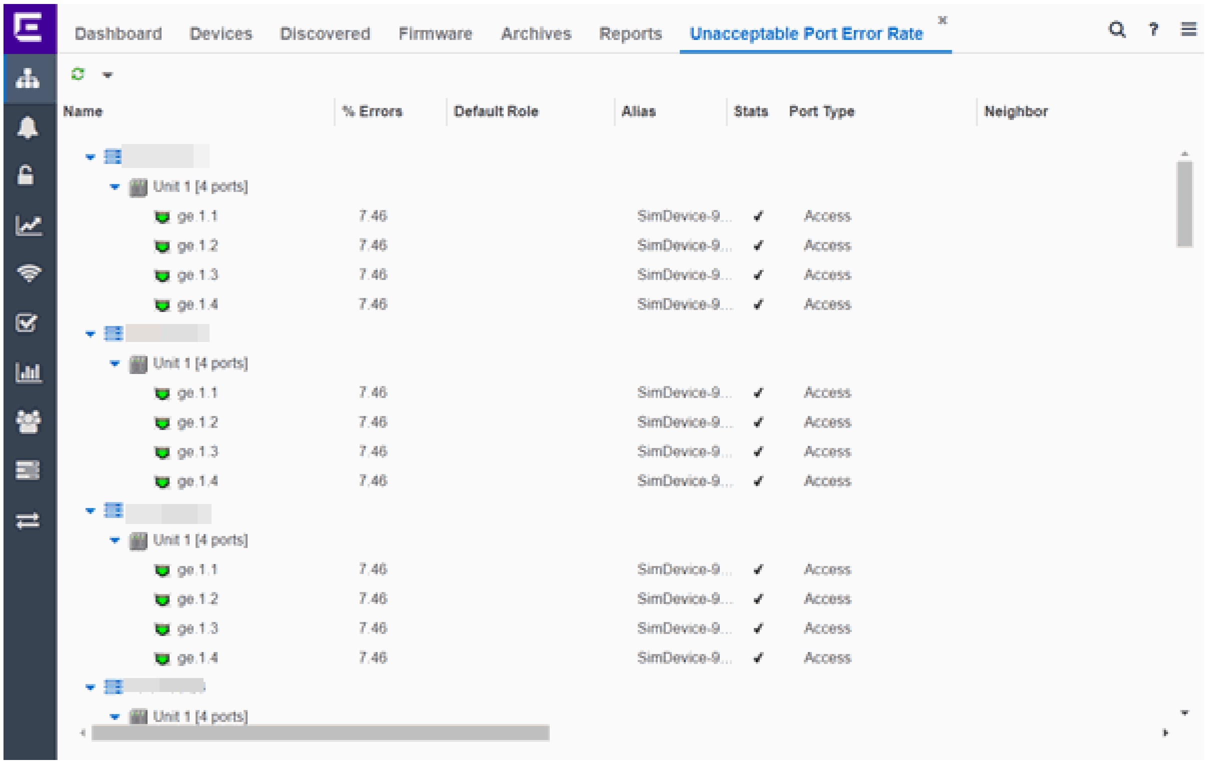
Related Information

- Impact Analysis Dashboard Overview

High Error Ports Report

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

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port error rates.



Name	% Errors	Default Role	Alias	Stats	Port Type	Neighbor
[redacted]						
Unit 1 [4 ports]						
ge.1.1	7.46		SimDevice-9...	✓	Access	
ge.1.2	7.46		SimDevice-9...	✓	Access	
ge.1.3	7.46		SimDevice-9...	✓	Access	
ge.1.4	7.46		SimDevice-9...	✓	Access	
[redacted]						
Unit 1 [4 ports]						
ge.1.1	7.46		SimDevice-9...	✓	Access	
ge.1.2	7.46		SimDevice-9...	✓	Access	
ge.1.3	7.46		SimDevice-9...	✓	Access	
ge.1.4	7.46		SimDevice-9...	✓	Access	
[redacted]						
Unit 1 [4 ports]						
ge.1.1	7.46		SimDevice-9...	✓	Access	
ge.1.2	7.46		SimDevice-9...	✓	Access	
ge.1.3	7.46		SimDevice-9...	✓	Access	
ge.1.4	7.46		SimDevice-9...	✓	Access	
[redacted]						
Unit 1 [4 ports]						

The following columns are included in the report:

Name

The device or port interface name.

% Errors

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

Default Role

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

Alias

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

Stats

Displays information about the port, if configured in PortView.

Port Type

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

Neighbor

The port to which the port is connected.

Port Speed

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

PVID

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

VLANs

The VLANs to which the port is associated.

Description

A description of the port and the device.

Port Type Details

Additional information about the type of port.

Serial Number

The serial number of the device.

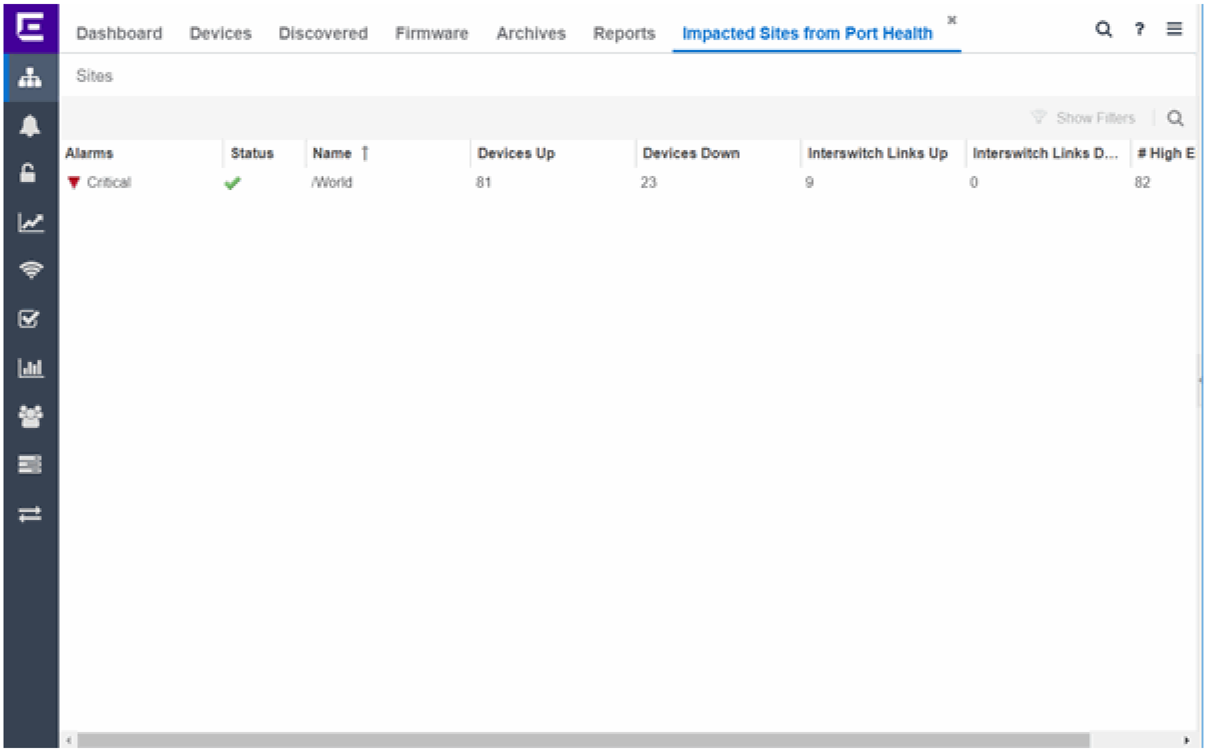
Related Information

- Impact Analysis Dashboard Overview

Sites Impacted by High Error Ports Report

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

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port error rates.



Alarms	Status	Name	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links D...	# High E
▼ Critical	✓	/World	81	23	9	0	82

The following columns are included in the report:

Alarms

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

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

Status

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

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

Name

The name of the site.

Devices Up

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

Devices Down

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

Interswitch Links Up

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

Interswitch Links Down

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

# High Error Rate Ports

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

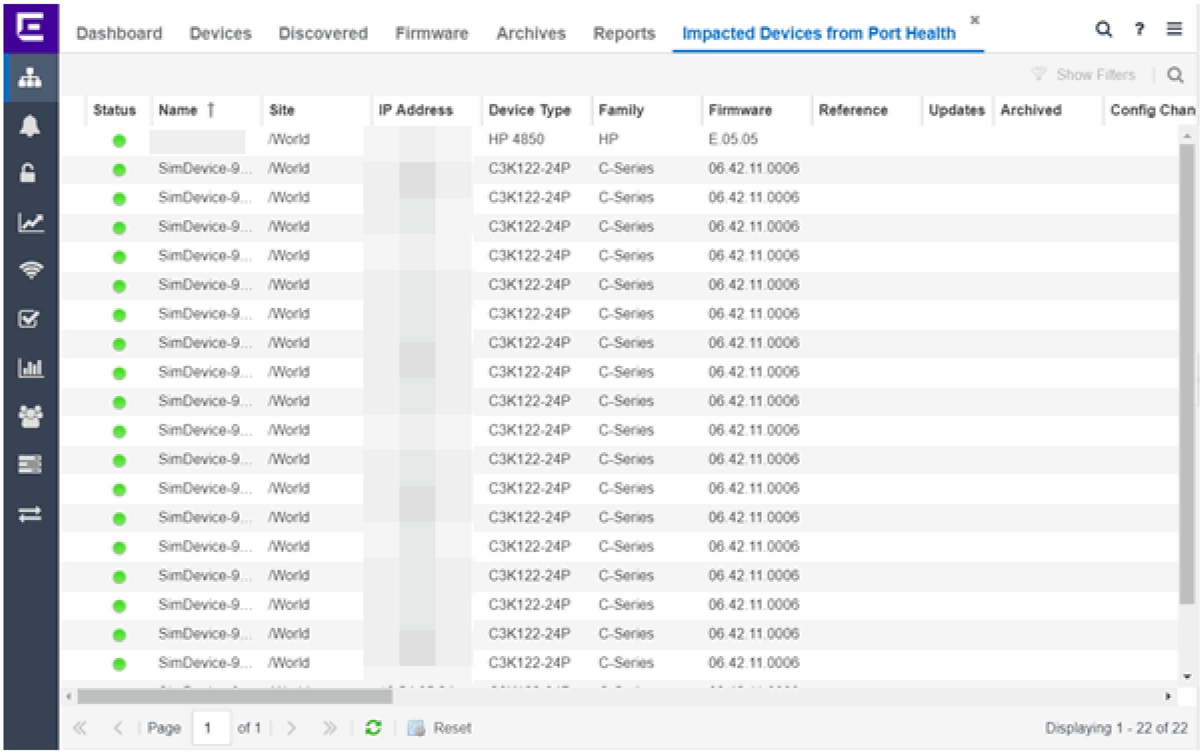
Related Information

- Impact Analysis Dashboard Overview

Devices Impacted by High Error Ports Report

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

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port error rates.



Status	Name	Site	IP Address	Device Type	Family	Firmware	Reference	Updates	Archived	Config Chan
●	[redacted]	/World	[redacted]	HP 4850	HP	E.05.05				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				
●	SimDevice-9...	/World	[redacted]	C3K122-24P	C-Series	06.42.11.0006				

The following columns are included in the report:

Device Status

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

- Green icon (●) — Indicates Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center can not contact the device.

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

Status

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

- Red icon (▼) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.

- Yellow icon (▲) — A warning that might lead to a problem.
- Blue icon (🟦) — Information only; not a problem.
- Green icon (🟢) — Extreme Management Center can contact the device.

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

Device ID

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

Name

The device name, nickname, or IP address.

Site

The site in which the device is located.

Poll Type

This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name

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

Admin Profile

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

Client Profile

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

IP Address

The device's IP address.

Context

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

IP Context

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

Trap Status

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

Syslog Status

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

Display Name

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

Device Type

The type of device.

Family

The device product family.

Firmware

The revision for the firmware running in the device.

Running Reference Firmware

Indicates if the device is running reference firmware.

Updates

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

Archived

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

Config Changed

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

Policy Domain

The policy domain assigned to the device.

Boot PROM

The revision for the BootPROM installed on the device.

Base MAC

The base MAC address for the device.

Serial Number

The serial number for the device.

Stats

Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.

Location

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

Contact

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

System Name

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

Uptime

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

Nickname

The user-defined nickname for the selected device.

Description

A description of the unavailable device.

User Data 1-4, Notes

These columns can provide additional information about the device.

Asset Tag

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

Related Information

- Impact Analysis Dashboard Overview

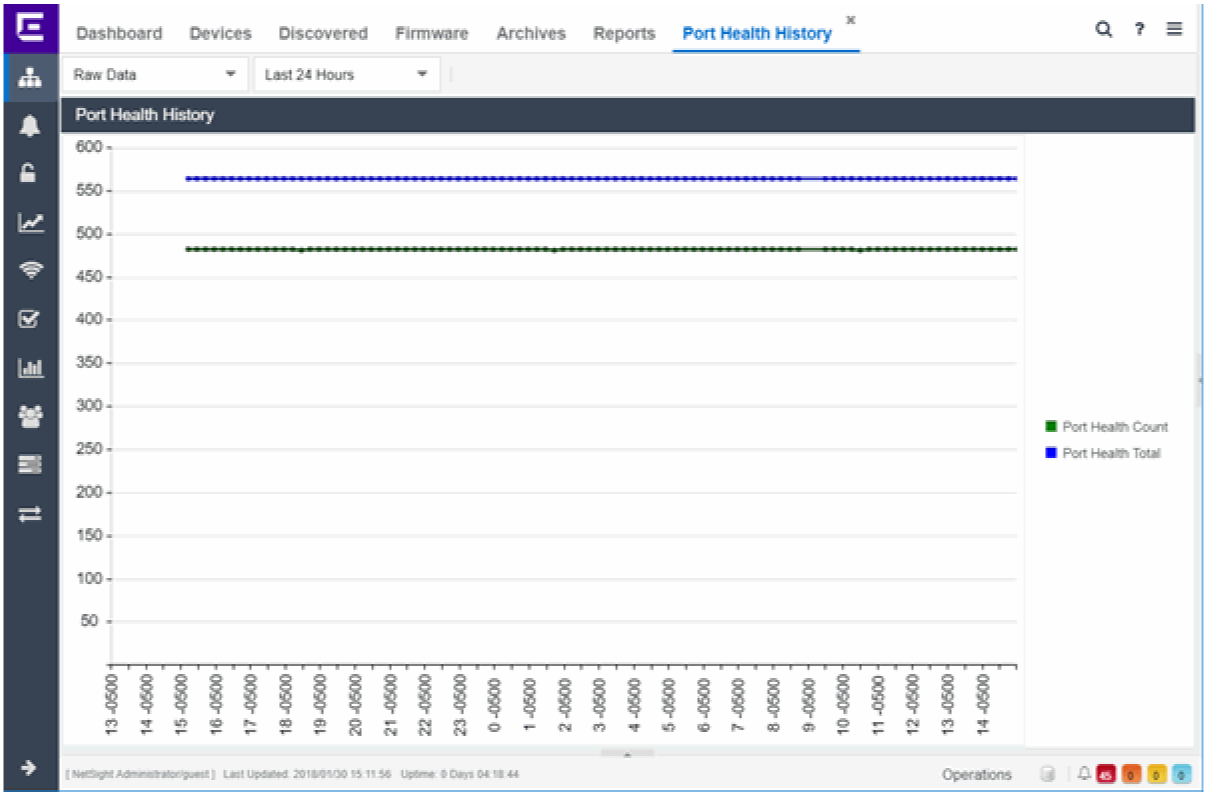
Port Health History Report

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

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold Extreme Management Center uses to determine port error rates.

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

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

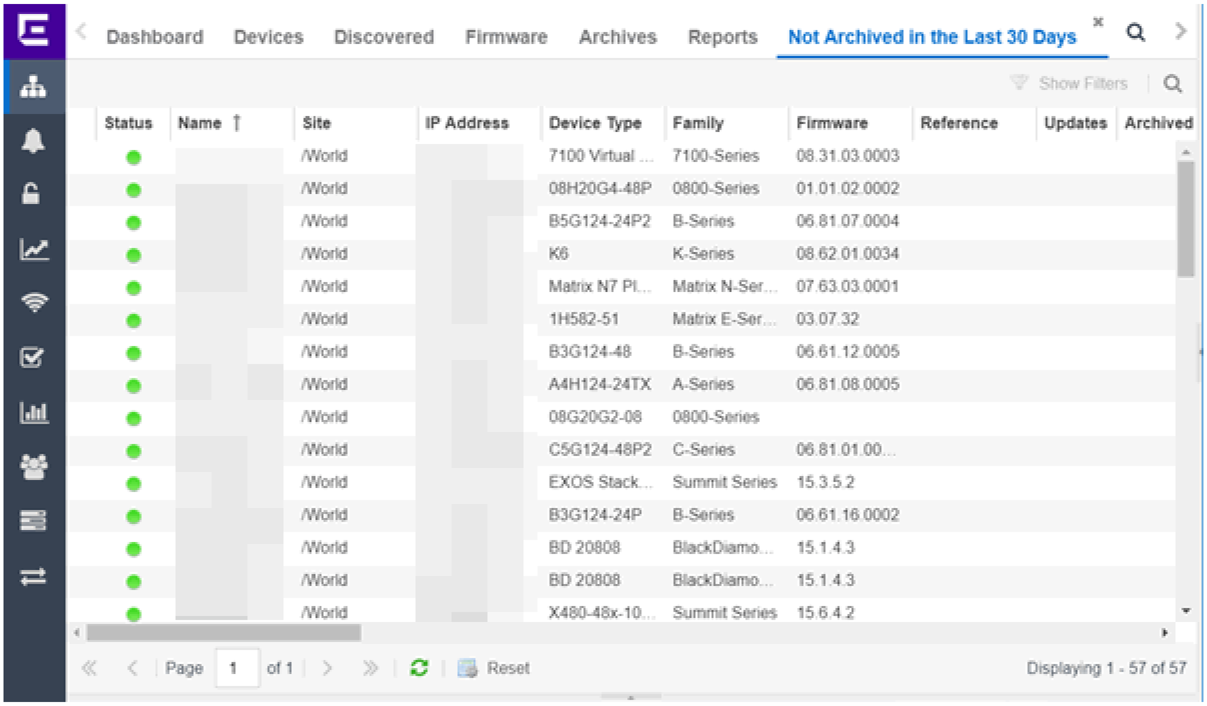


Related Information

- Impact Analysis Dashboard Overview

Unarchived Devices Report

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



Status	Name	Site	IP Address	Device Type	Family	Firmware	Reference	Updates	Archived
●		/World		7100 Virtual ...	7100-Series	08.31.03.0003			
●		/World		08H20G4-48P	0800-Series	01.01.02.0002			
●		/World		B5G124-24P2	B-Series	06.81.07.0004			
●		/World		K6	K-Series	08.62.01.0034			
●		/World		Matrix N7 Pl...	Matrix N-Ser...	07.63.03.0001			
●		/World		1H582-51	Matrix E-Ser...	03.07.32			
●		/World		B3G124-48	B-Series	06.61.12.0005			
●		/World		A4H124-24TX	A-Series	06.81.08.0005			
●		/World		08G20G2-08	0800-Series				
●		/World		C5G124-48P2	C-Series	06.81.01.00...			
●		/World		EXOS Stack...	Summit Series	15.3.5.2			
●		/World		B3G124-24P	B-Series	06.61.16.0002			
●		/World		BD 20808	BlackDiamo...	15.1.4.3			
●		/World		BD 20808	BlackDiamo...	15.1.4.3			
●		/World		X480-48x-10...	Summit Series	15.6.4.2			

The following information is included in the report:

Device Status

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

- Green icon (●) — Indicates Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center can not contact the device.

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

Status

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

- Red icon (▼) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.
- Yellow icon (▲) — A warning that might lead to a problem.

- Blue icon (🟦) — Information only; not a problem.
- Green icon (🟢) — Extreme Management Center can contact the device.

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

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

Name
The device name, nickname, or IP address.

Site
The site in which the device is located.

Poll Type
This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.

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

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

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

IP Address
The device's IP address.

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

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

Trap Status

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

Syslog Status

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

Display Name

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

Device Type

The type of device.

Family

The device product family.

Firmware

The revision for the firmware running in the device.

Running Reference Firmware

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

Updates

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

Archived

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

Config Changed

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

Policy Domain

The policy domain assigned to the device.

Boot PROM

The revision for the BootPROM installed on the device.

Base MAC

The base MAC address for the device.

Serial Number

The serial number for the device.

Stats

Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.

Location

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

Contact

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

System Name

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

Uptime

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

Nickname

The user-defined nickname for the selected device.

Description

A description of the unavailable device.

User Data 1-4, Notes

These columns can provide additional information about the device.

Asset Tag

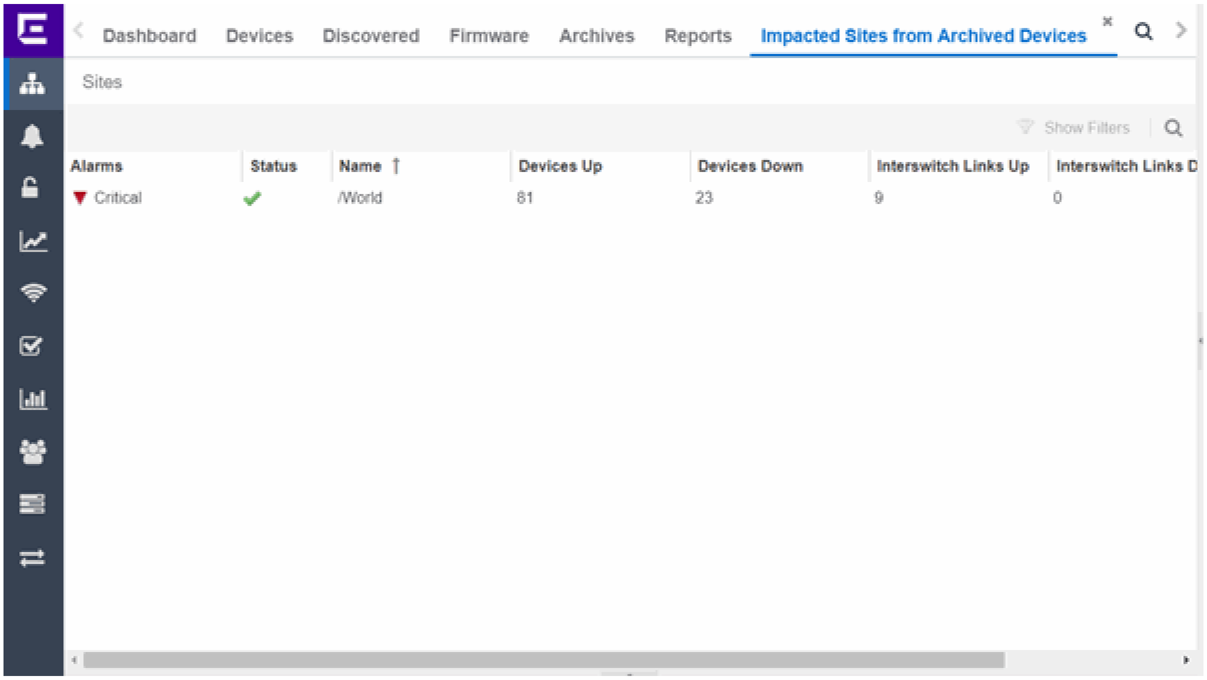
A unique asset number assigned to the module or component for inventory tracking purposes.

Related Information

- Impact Analysis Dashboard Overview

Sites Impacted by Unarchived Devices Report

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



Alarms	Status	Name ↑	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links D
▼ Critical	✓	/World	81	23	9	0

The following columns are included in the report:

Alarms

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

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

Status

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

down.

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

Name

The name of the site.

Devices Up

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

Devices Down

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

Interswitch Links Up

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

Interswitch Links Down

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

# Unarchived Devices

The number of devices not archived in the last 30 days in the site.

Related Information

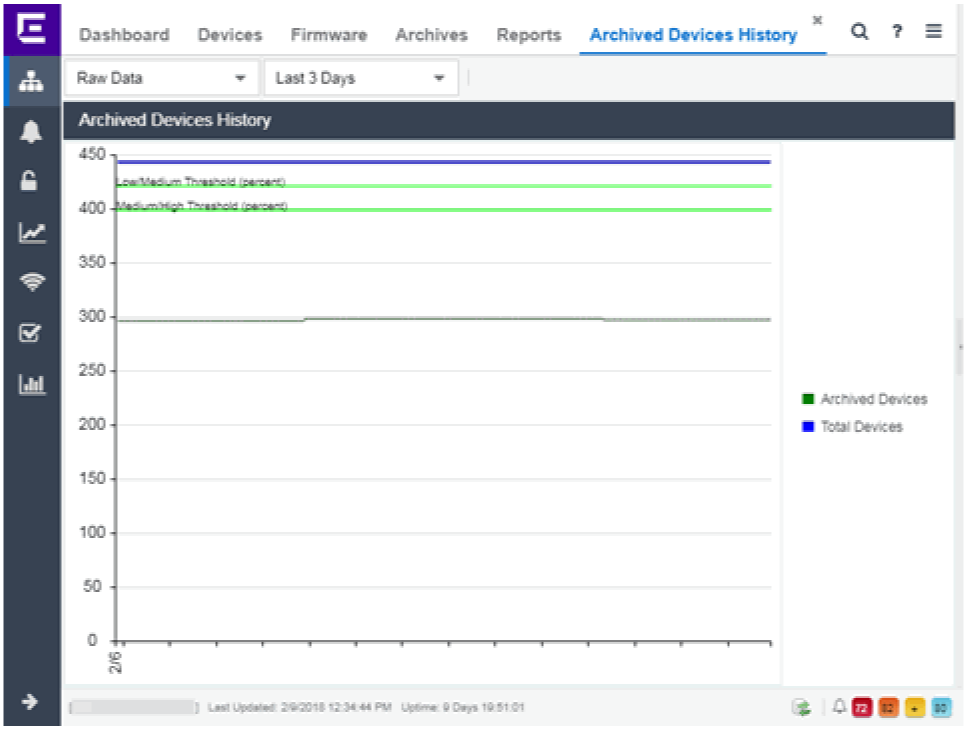
- Impact Analysis Dashboard Overview

Archived Devices History Report

The Archived Devices History report contains a graph that displays the number of devices archived within the last 30 days (green) and the total number of devices that can be archived (blue) for the duration you define. If no devices have been archived in the last 30 days, the chart may not display data (green). The values here are the values displayed in the Archived Devices ring chart over the time span you define.

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

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

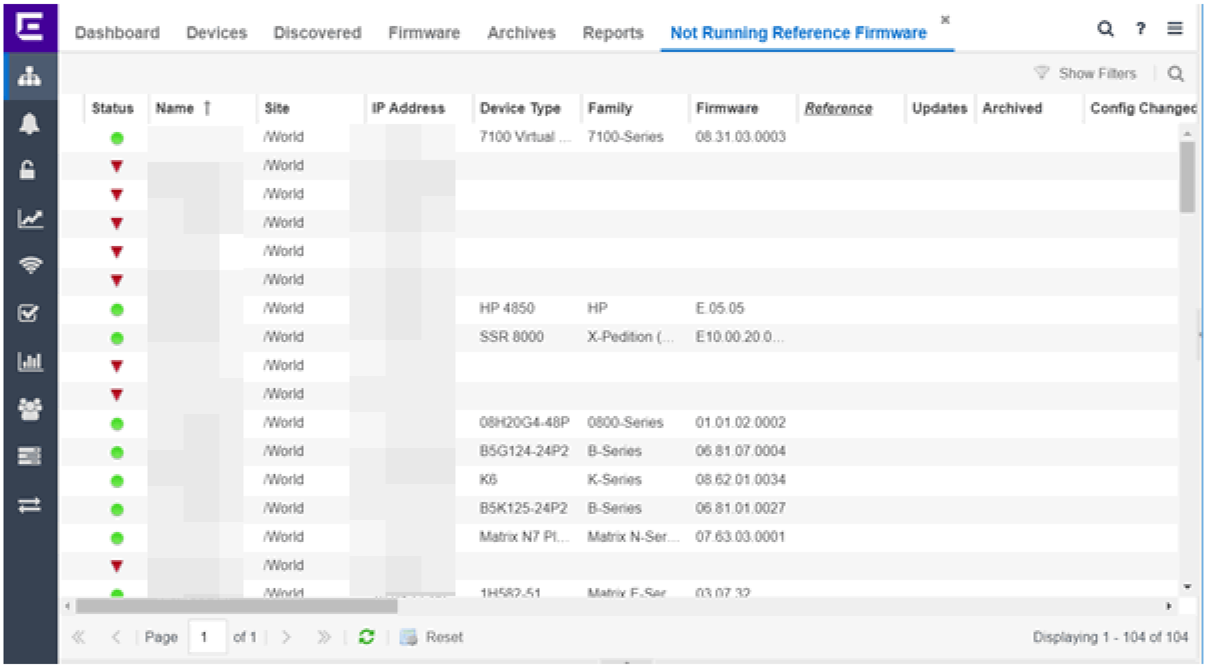


Related Information

- Impact Analysis Dashboard Overview

Devices Without Reference Firmware Report

The Devices Without Reference Firmware report provides detailed information about devices not running reference firmware.



Status	Name	Site	IP Address	Device Type	Family	Firmware	Reference	Updates	Archived	Config Changed
●		/World		7100 Virtual ...	7100-Series	08.31.03.0003				
▼		/World								
▼		/World								
▼		/World								
▼		/World								
▼		/World								
●		/World		HP 4850	HP	E.05.05				
●		/World		SSR 8000	X-Pedition (...	E10.00.20.0...				
▼		/World								
▼		/World								
●		/World		08H20G4-48P	0800-Series	01.01.02.0002				
●		/World		B5G124-24P2	B-Series	06.81.07.0004				
●		/World		K6	K-Series	08.62.01.0034				
●		/World		B5K125-24P2	B-Series	06.81.01.0027				
●		/World		Matrix N7 Pl...	Matrix N-Ser...	07.63.03.0001				
▼		/World								
●		/World		1H582-51	Matrix E-Ser	03.07.32				

Page 1 of 1 | Reset | Displaying 1 - 104 of 104

The following columns are included in the report:

Device Status

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

- Green icon (●) — Indicates Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center can not contact the device.

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

Status

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

- Red icon (▼) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.
- Yellow icon (▲) — A warning that might lead to a problem.

- Blue icon (🟦) — Information only; not a problem.
- Green icon (🟢) — Extreme Management Center can contact the device.

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

Device ID

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

Name

The device name, nickname, or IP address.

Site

The site in which the device is located.

Poll Type

This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name

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

Admin Profile

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

Client Profile

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

IP Address

The device's IP address.

Context

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

IP Context

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

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

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

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

Device Type
The type of device.

Family
The device product family.

Firmware
The revision for the firmware running in the device.

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

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

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

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

Policy Domain
The policy domain assigned to the device.

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

Base MAC
The base MAC address for the device.

Serial Number

The serial number for the device.

Stats

Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.

Location

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

Contact

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

System Name

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

Uptime

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

Nickname

The user-defined nickname for the selected device.

Description

A description of the unavailable device.

User Data 1-4, Notes

These columns can provide additional information about the device.

Asset Tag

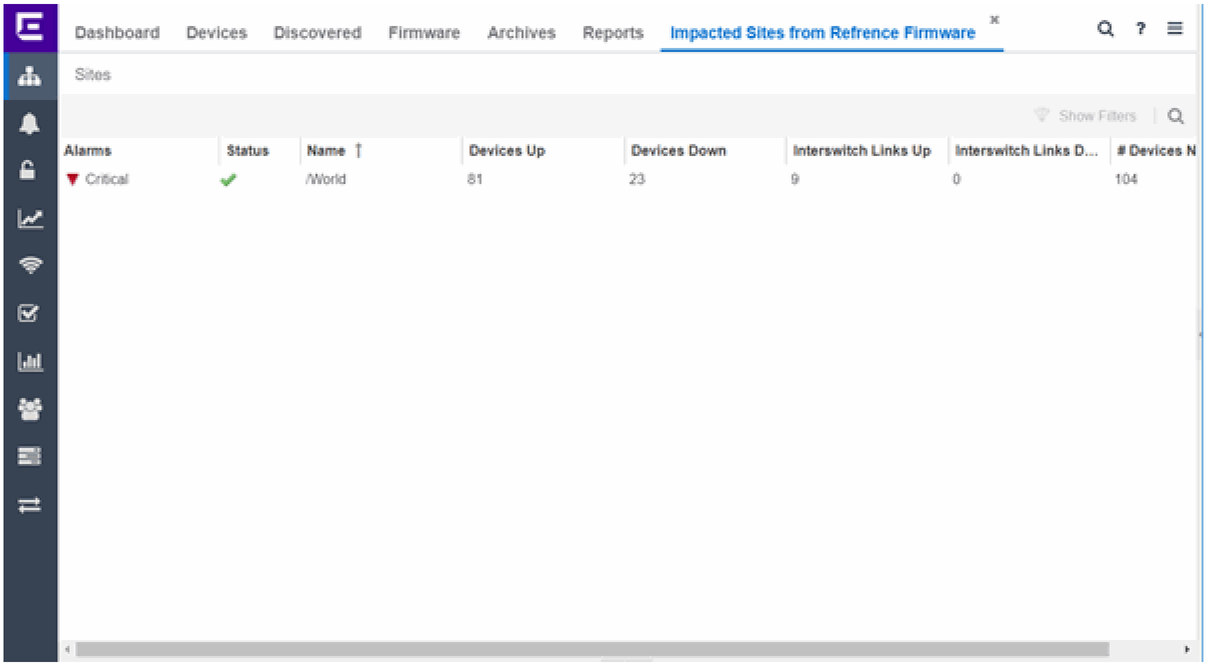
A unique asset number assigned to the module or component for inventory tracking purposes.

Related Information

- Impact Analysis Dashboard Overview

Sites Impacted by Devices Without Reference Firmware Report

This report provides a list of sites with devices not running reference firmware.



Alarms	Status	Name ↑	Devices Up	Devices Down	Interswitch Links Up	Interswitch Links D...	# Devices N
▼ Critical	✓	/World	81	23	9	0	104

The following columns are included in the report:

Alarms

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

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

Status

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

down.

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

Name
The name of the site.

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

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

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

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

# Devices Not Running Reference Firmware
The number of devices not running reference firmware in the site.

Related Information

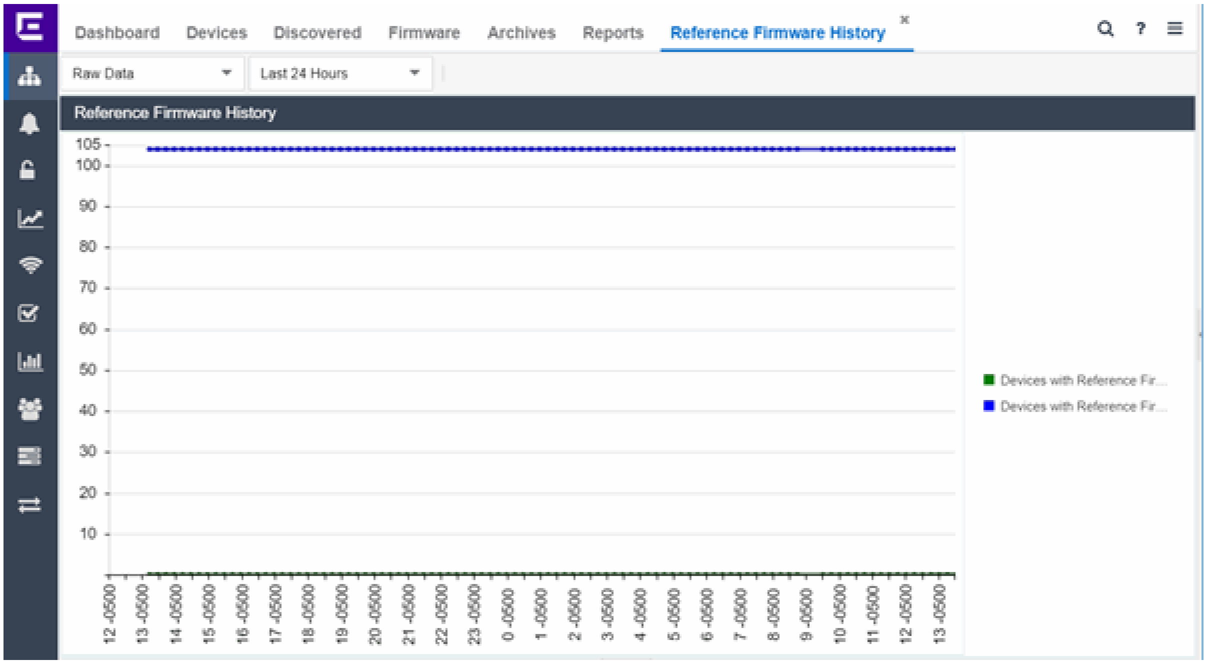
- Impact Analysis Dashboard Overview

Reference Firmware History Report

The Reference Firmware History Report displays the number of devices running reference firmware (green) and the total number of devices (blue) for the duration you define. If no devices are running reference firmware, the chart may not display data (green). The values here are the values displayed in the Devices with Reference Firmware ring chart over the time span you define.

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

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



Related Information

- Impact Analysis Dashboard Overview

Device Operations

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

- Add Device
- Configure Device
- Execute CLI Commands
- Delete Device
- Set Profile
- Create Device Group
- Add Devices to a Device Group

- Backup, Restore, and Compare Device Configurations
- View Port Tree
- View Interface Summary
- View FlexViews
- View User Sessions
- Authentication Configuration
- Launch WebView
- View Network Details
- Collect Device Statistics
- Upgrade Firmware
- Register Trap Receiver
- Unregister Trap Receiver
- Register SysLog Receiver
- Unregister SysLog Receiver
- View Device Details
- Create and Edit Maps
- Add Devices to Maps
- View and Set Policy
- Manage Device Serial Numbers
- Run Tasks on Devices, Ports, and Groups
- Working in the Devices Table
    - Set Device Values
    - Table Column Definitions
- Filtering
- Buttons, Search Field, and Paging Toolbar
- Local Settings

To view the **Devices** sub-tab on the **Network** tab, you must be a member of an authorization group assigned the OneView > Access OneView and the OneView > Events and Alarms > OneView Event Log Access capabilities.

Add Device

To add a new device to the Devices list:

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

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

Configure Device

To configure device information for an existing device:

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

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

Execute CLI Commands

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

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

The **Execute CLI Commands** window opens, from which you can enter the commands and execute on the devices you select. Click the **Launch** link at the top of the window in the **Termial Window** column to test the credentials and view the results in the **Results** tab at the bottom of the window.

NOTE: Commands you define are run on all of the devices displayed at the table at the top of the window.

Delete Device

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

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

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

Set Profile

To change the profile settings for a device or multiple devices from the Devices list:

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

   The Set Profile window appears.
4. Select a profile from the drop-down menu to change the profile for the selected device or devices.
5. Click **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 in the Groups/Maps left-panel and select **Device Groups** > **Create Device Group**.

   The Add Device Group window appears.

2. Enter a name for the device group.
3. Click **OK**.

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

Add Devices to a Device Group

To add a device or multiple devices to a device group:

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

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

Back up, Restore, and Compare Device Configurations

You can back up (archive) and restore device configurations as well as compare two configuration files, using the **Network** tab in Extreme Management Center.

View Port Tree

The Port Tree displays interface information for a device.

To open the Port Tree:

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

   The Port Tree opens in a new tab.
5. Expand the components to see the device's interfaces. Right-click on an interface to:

- access PortView for that interface
- view interface history including interface utilization, availability, and bandwidth/packets/flows statistics
- run scripts on the selected port
- enable interface statistic collection
- create policy profiles, called roles, that are assigned to the ports in your network.

In the Port Tree table, the Stats column displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, a blue check indicates that monitor collection is enabled. The Neighbor column displays neighbor details from CDP/EDP/LLDP. Hover your mouse over the column to see the protocol type.

View Interface Summary

From the Interface Summary, you can right-click on an interface to access PortView, view interface history, view current alarms and alarm history, enable interface statistic collection, and edit certain values for an interface.

To open the Interface Summary:

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

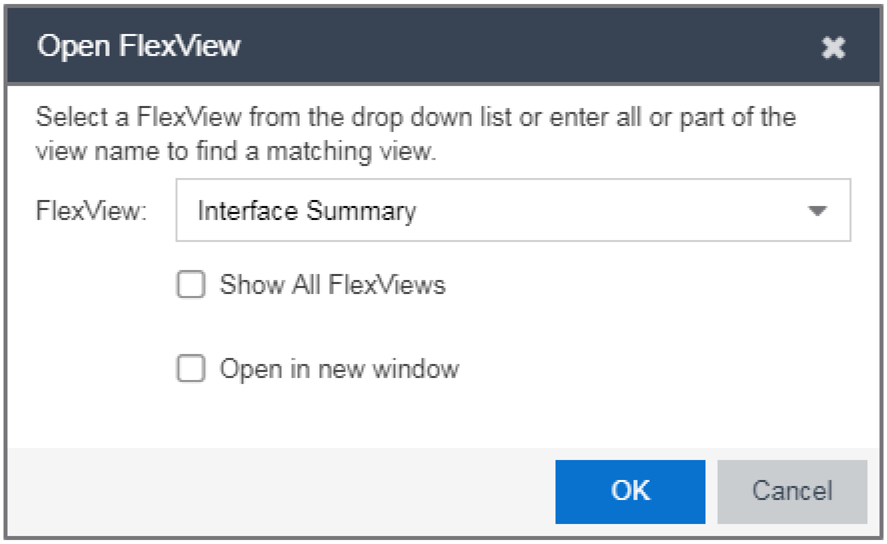
   An Interface Summary FlexView opens for the device in a new tab.

View FlexViews

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

To launch a FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a web-based FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

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



Open FlexView

Select a FlexView from the drop down list or enter all or part of the view name to find a matching view.

FlexView: Interface Summary

□ Show All FlexViews

□ Open in new window

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

For additional information about launching and using FlexViews from the **Network** tab, see Web-Based FlexViews.

View User Sessions

You can use the **Network** tab to view user sessions associated with the selected device.

To launch the user session, you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session

Read Access capability. To launch and edit a User Session , you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session Read/Write Access capability.

To open a user session for a device, select a device in the Device list, click the **Menu** icon (☰) or right-click in the Devices list to select **View** > **User Session** from the menu. You can also right-click on a device and select **View** > **User Session** from the menu. In the User Sessions window, you can view all users accessing the device selected.

For additional information about the User Sessions window, see User Sessions.

Authentication Configuration

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

Launch WebView

You can use the **Network** tab to access WebView web-based management, which lets you configure and manage certain Extreme Networks and Enterasys devices.

To open WebView, select a device in the Device list, click the **Menu** icon (☰) or right-click in the Devices list to select **View** > **Device Details** > **Launch WebView** from the menu.

The web-based management opens in a new browser window. If your authorization group has been assigned the capability for Suite > Device Local Management WebView, you can take advantage of the auto login feature for web local management of Extreme Access Control engines and wireless controllers.

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

View Network Details

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

To open the Network Details:

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

   The tabs at the bottom of the window populate with information about the connection you select. All connections managed by Extreme Management Center are available. You can also view the Network Details for connections included in a specific Map by opening the Map and selecting one of the tabs in the Network Details section of the window. Selecting a connection listed on the tab highlights the connection on the map.

Collect Device Statistics

The **Network** tab provides the ability to start and stop device statistics collections for Extreme Networks and Enterasys devices, which allows the collection of data used in reports.

To collect device statistics:

1. Select one or more devices or wireless controllers in the Device list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select one of the following menu options from within the Device submenu:
   - **Collect Device Statistics** — Opens a window that allows you to enable or disable Historical or Monitor statistics collection mode.
     - In **Historical mode**, device and physical port statistics are saved to the database and aggregated over time, for use in reports. The device statistics are also used for threshold alarms configured in the Console Alarms Manager. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the Console Alarms Manager that use these statistics.

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

     - In **Monitor mode**, device statistics are saved to a Monitor cache for one hour and then dropped. You can use these statistics for threshold alarms, but not for Extreme Management Center reporting. In the Active

Threshold Alarm Summary box, you can see all active threshold alarms configured in the **Alarms and Events** tab that use these statistics. (Note that you do not see the Monitor mode option if you have disabled Monitor Collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)

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

4. If you are enabling statistics collection on an Extreme Access Control engine, Application Analytics engine, or ExtremeWireless Controller, read through the following notes:
   - **Extreme Access Control Engine** — When collecting statistics on an Extreme Access Control engine, the active engine must be added to Extreme Management Center to collect all appliance statistics. In addition, Monitor mode is not supported on Extreme Access Control engines.
   - **Application Analytics Engine** — When collecting statistics on an Application Analytics engine, the engine must be added to the **Analytics** > **Configuration** > Application Analytics Engines table in order for Extreme Management Center to collect all Application Detection statistics. In addition, Monitor mode is not supported on Application Analytics engines.
   - **ExtremeWireless Controller** — Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

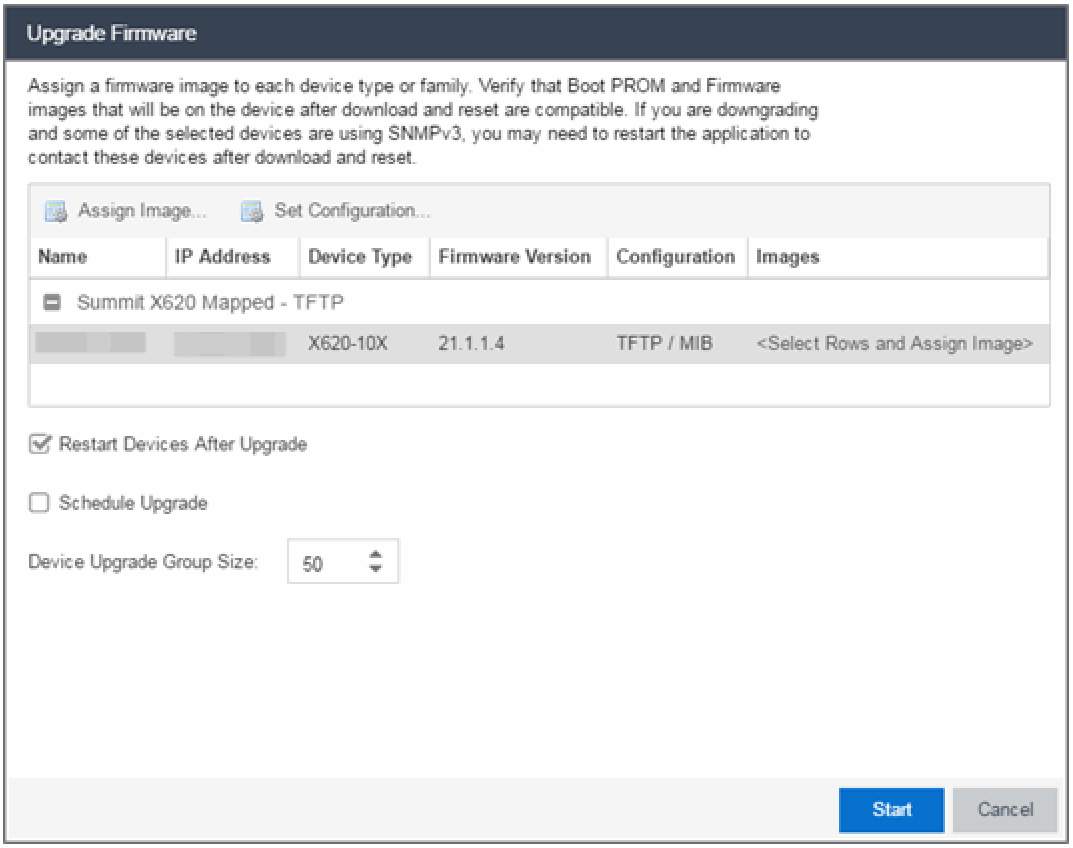
For additional information about collecting statistics, see Enable Report Data Collection.

Open Device Terminal

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

Upgrade Firmware

To update devices in the Extreme Management Center database with the latest firmware releases, click the **Menu** icon (≡) or right-click in the Devices list and select **Configuration/Firmware** > **Upgrade Firmware**. The results display in the Upgrade Firmware window with displaying information about the device and the available firmware versions. For additional information about upgrading device firmware, see How to Upgrade Firmware. Restart devices once the firmware is upgraded via the Restart Devices window by selecting **Configuration/Firmware** > **Restart Device**.


Upgrade Firmware

Assign a firmware image to each device type or family. Verify that Boot PROM and Firmware images that will be on the device after download and reset are compatible. If you are downgrading and some of the selected devices are using SNMPv3, you may need to restart the application to contact these devices after download and reset.

Name	IP Address	Device Type	Firmware Version	Configuration	Images
⊟ Summit X620 Mapped - TFTP					
[redacted]	[redacted]	X620-10X	21.1.1.4	TFTP / MIB	<Select Rows and Assign Image>

☑ Restart Devices After Upgrade

☐ Schedule Upgrade

Device Upgrade Group Size: 50

Register Trap Receiver

To receive trap information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Register Trap Receiver** from the menu. Additionally, devices added to sites for which **Add Trap Receiver** is selected on the Discovered Device Actions tab automatically receive trap information. You can define the trap configuration details on the

Options > Trap tab. Depending on the device, Extreme Management Center creates the trap configuration via SNMP or a script.

Unregister Trap Receiver

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

Register SysLog Receiver

To receive syslog information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Register SysLog Receiver** from the menu. Additionally, devices added to sites for which **Add Syslog Receiver** is selected on the Discovered Device Actions tab automatically receive syslog information. You can define the syslog configuration details on the **Options** > Syslog tab. Depending on the device, Extreme Management Center creates the syslog configuration via SNMP or a script.

Unregister SysLog Receiver

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

View Device Details

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

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

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

Create and Edit Maps

Maps visually organize the devices on your network, based on their geographic location or based on the other devices to which they connect.

You can create a new map by either clicking the **Menu** icon (≡) or right-click in the World map navigation tree and selecting **Maps** > **Create New Map**.

You can also create a map for a specific device or device group by selecting the device or device group in the Device Groups navigation tree in the Devices section of the window or in the Devices list and selecting **Maps** > **Create New Map**. For additional information, see Create and Edit Maps.

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

Add Devices to Maps

To add a device to an existing map:

1. Select one or more devices in the Device list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Maps** > **Add to Map**.

   For additional information, see Create and Edit Maps.

To add devices or APs to new maps:

1. Select one or more devices in the Device list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Maps** > **Create Maps For Locations**.

   For additional information, see Create and Edit Maps.

View and Set Policy

You can use the **Network** tab to access a Policy menu, which lets you view and set policy for a device or port.

To view or set policy for a device:

1. Select one or more devices in the Devices table.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Open the Policy menu to view the currently assigned domain, change domain assignment, set or clear the default role for all ports, or Enforce or Verify the domain.

To view or set policy for a port:

1. Click the **Menu** icon (≡) or right-click in the Devices list.
2. Select **View** > **Port Tree**.
3. Select one or more ports.
4. Right-click and use the Policy menu to view the currently assigned domain, set or clear the port default role, and see role details for the default role.

If the device doesn’t support policy or isn’t assigned to a domain, the Port Tree Policy menu options are grayed out and you see either "Policy Unsupported" or "Current Domain: Unassigned". If the domain is unassigned, you must first assign the device to a domain before you can access Policy menu options in the Port Tree.

Manage Device Serial Numbers

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

To register or export your network device serial number:

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

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

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

Run Tasks on Devices, Ports, and Groups

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

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

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

Working in the Devices List

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

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

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

Set Device Values

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

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

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

Devices List Column Definitions

- DeviceView ▼ — Hover your mouse over the first column and click on the icon to open a DeviceView that provides analysis and troubleshooting information for the selected device, including device summary, FlexView, and Extreme Management Center historical data. You must have historical statistic collection enabled for the device to see data for the full range of available reports. For more information, see Collect Device Statistics.
- Device Status — This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating. A green icon indicates there is contact with the device. A yellow icon indicates there are issues with contact to the device. A red icon indicates there is no contact with the device. Hover over the Device Status icon to view additional details about the status for that device.
- Status — Indicates the alarm/device status for the device. The colored circle indicates the severity of the most severe alarm on the device. A green icon indicates that there are no alarms and the device is up. A red icon indicates a critical alarm or the device is down. Hover over the status icon to view the number of alarms. Click on the alarm/device status icon to open a new page with detailed information about the alarms for that device.
- Device ID — This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.
- Name — The device name or nickname, or IP address. Click on the link to open an Interface Summary FlexView for the device.

- Poll Type — This column, hidden by default, indicates the poll type Extreme Management Center uses to discover devices: SNMP, Ping or Not Polled.
- Poll Group Name — This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.
- Admin Profile — This column, hidden by default, indicates the access Profile that gives Extreme Management Center administrative access to the device.
- Client Profile — This column, hidden by default, indicates the access Profile that gives Extreme Management Center client access to the device.
- IP Address — The device IP address. This column is hidden by default.
- Context — The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.
- IP Context — The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.
- Trap Status — Indicates whether a trap receiver is configured, not configured, or not supported for the device.
- Syslog Status — Indicates whether the device is configured to send information to the syslog or if it is not supported for the device.
- Display Name — The IP address of the device. This column is hidden by default.
- Device Type — The type of device.
- Family — The device product family.
- Firmware — The revision for the firmware running in the device.
- Updates — The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.
  - Firmware Up To Date — The device is running the latest release of firmware.
  - New Firmware Release Available — There is a new release of firmware available for this device. Click the **Menu** icon (≡) or right-click the icon and select **Configuration/Firmware** > **View Available Releases** to open a window listing the current firmware releases available with links to download the firmware.
  - Run 'Check for Updates' to find new firmware releases — A Check for Firmware Updates needs to be performed to get updates for this device. Click the **Menu** icon (≡) or right-click the device and select **Configuration/Firmware > Check for Updates** from the menu.

    - Device does not support Firmware Updates feature — This device does not support the Check for Firmware Updates feature.
- **Policy Domain — The policy domain assigned to the device.**
- BootPROM — The revision for the BootPROM installed on the device.
- Base MAC — The base MAC address for the device.
- Serial Number — The serial number for the device.
- Stats — Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that monitor collection is enabled.
- Location — The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.
- Contact — The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.
- System Name — An administratively-assigned hostname for the device taken from the *sysName* MIB object. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting Set System Name from the menu
- Uptime — The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.
- Nickname — The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when the Use User Defined Nickname option is selected in Console > Options > Console > How to display devices in the device tree. You can set the nickname for a device by selecting the device in the table, right-clicking in the Nickname column, and selecting Device > Set Nickname from the menu.
- Description — A description of the device.
- User Data 1-4, Notes — These columns can provide additional information about the device. You can set the user data and notes for one or more devices by selecting the devices in the table, right-clicking, and selecting Device > Set Selected User Data/Notes from the menu.

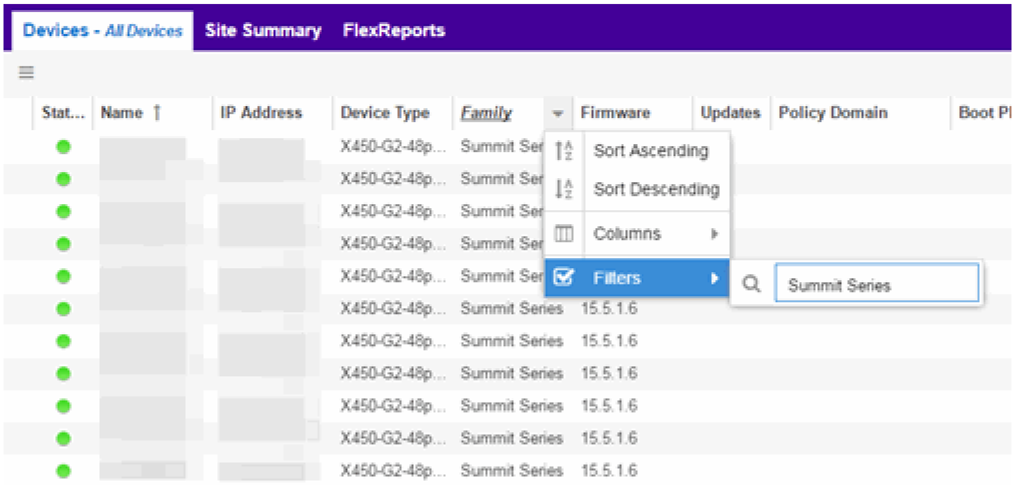
Filtering

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

Filter by String

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

Sample Filter by Family



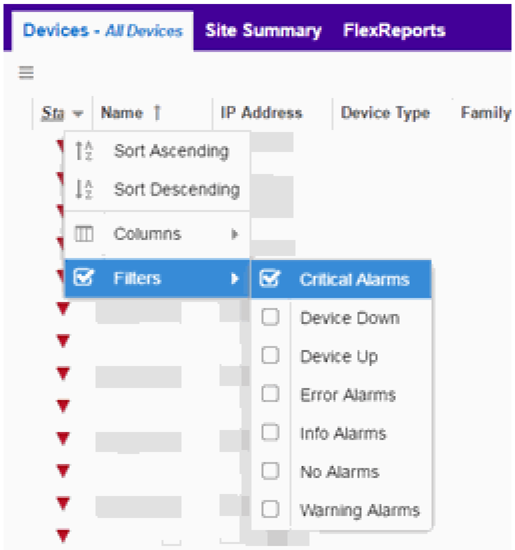
Summit Series

Stat...	Name	IP Address	Device Type	*Family*	Firmware	Updates	Policy Domain	Boot PI
●	[redacted]	[redacted]	X450-G2-48p...	Summit Ser				
●	[redacted]	[redacted]	X450-G2-48p...	Summit Ser				
●	[redacted]	[redacted]	X450-G2-48p...	Summit Ser				
●	[redacted]	[redacted]	X450-G2-48p...	Summit Ser				
●	[redacted]	[redacted]	X450-G2-48p...	Summit Ser				
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			
●	[redacted]	[redacted]	X450-G2-48p...	Summit Series	15.5.1.6			

Filter by List Choices

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

Sample Filter by Status Level



Buttons, Search Field, and Paging Toolbar

Show Filters

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

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

« ‹ Page 1 of 2 › »

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

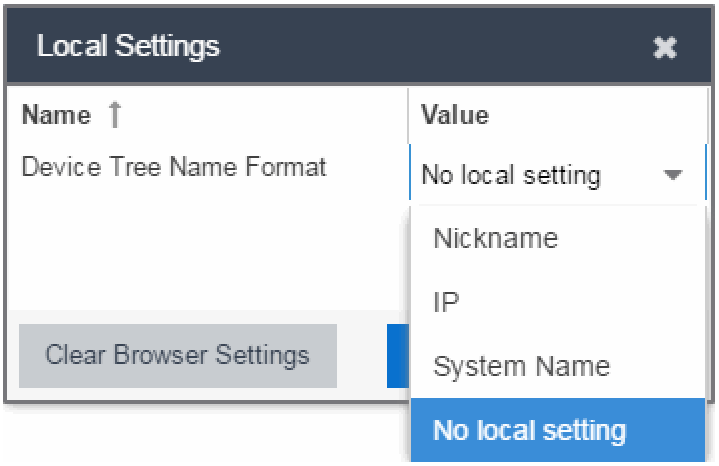
Clears the search field and search results, clears all filters, and refreshes the table.

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.



Local Settings

Name	Value
Device Tree Name Format	No local setting

- **Nickname** — Displays device names in the Device navigation tree using the Nickname entered when you added the device.
- **IP** — Displays device names in the Device navigation tree using the IP address of the device.
- **System Name** — Displays device names in the Device navigation tree using the system name of the device.

Additionally, clicking the **Clear Browser Settings** button changes the Extreme Management Center settings back to the system default.

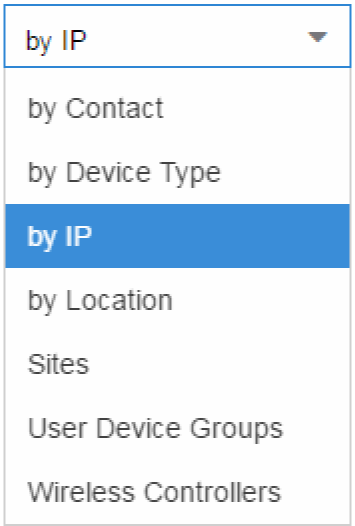
Related Information

For information on related topics:

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

Devices Navigation

The Extreme Management Center **Network** > **Devices** tab contains a left-panel drop-down menu that allows you to filter for devices by specific criteria, view all devices on your network, or select maps or sites.



Selecting an item in the drop-down menu filters the left-panel to display the devices, maps, or sites that apply to your selection.

by Contact
  Select **by Contact** to organize devices based on the Contact you configure on the **Configure Device** window.

by Device Type
  Select **by Device Type** to organize devices based on the type of device (e.g. Summit Series).

by IP

Select **by IP** to organize devices based on the IP address of your devices (e.g. all of the devices whose IP addresses begin with 10.20.30.x).

by Location

Select **by Location** to organize devices based on the Location you configure on the Configure Device window.

Sites

Select **Sites** to display all of your sites in the left-panel. A site is a group of devices that share a configuration. When a device is added to a site, Extreme Management Center configures the device to match the configuration of the site. Sites can also contain maps, which display devices based on their geographical or topological location. Devices that share connections or are located in a particular location display in the same map.

User Device Groups

Select **User Device Groups** to organize devices into device groups you create.

Wireless Controllers

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

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

Related Information

For information on related topics:

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

DeviceView

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

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

This Help topic provides the following DeviceView information:

- Requirements
  - Access Requirements
  - Data Collection Requirements
- DeviceView Reports
  - Left-Panel Device Summary
- Launching DeviceView

Requirements

Access Requirements

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

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

Data Collection Requirements

DeviceView reports require that historical data collection is enabled for the device. For information on configuring data collection, see Collect Device Statistics in the Devices section of the Extreme Management Center User Guide.

DeviceView Reports

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

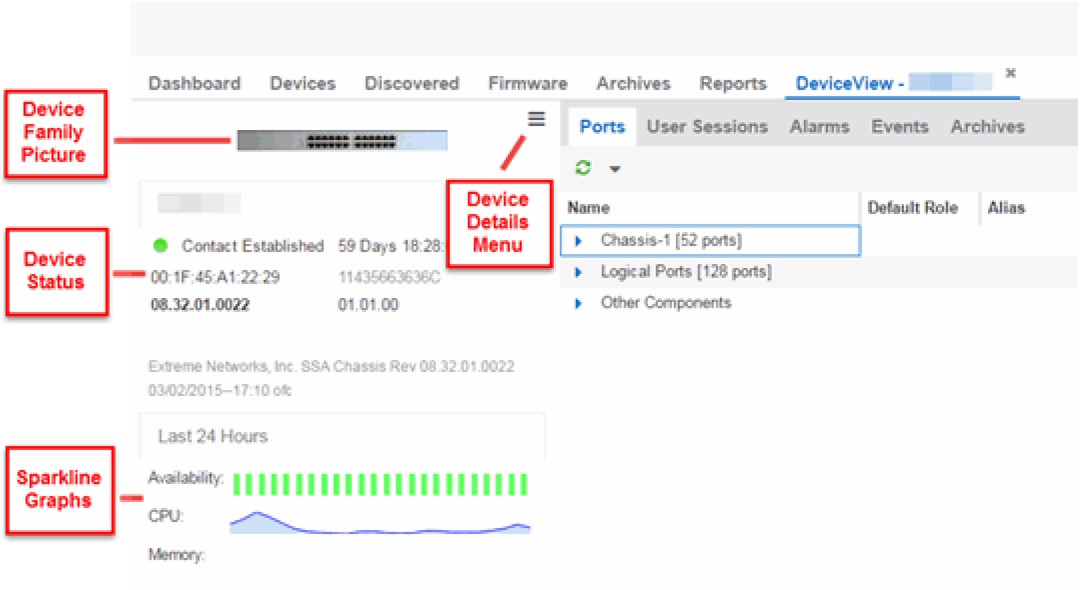
The following table shows the reports available for EOS devices, ExtremeXOS devices, and wireless controllers. The reports displayed in a DeviceView vary according to the selected device.

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

*Includes N-Series, S-Series, and K-Series devices.
**Includes BlackDiamond, E4G, and Summit Series devices.
***Right-clicking ports and selecting Add to Device Group opens the Add to Device Group window, which allows you to select a device group to which to add the selected ports.
****Only VLANs to which ports are assigned are displayed in this report. Additionally, VLAN reports for ExtremeXOS devices may display duplicate VLANs as VLANs are assigned by slot.

Left-Panel Device Summary

The left-panel device summary view (shown below) is displayed in each DeviceView report.



Each device summary view includes:

- Device Family Picture — A generic device family picture for the device.
- Device Status — Indicates the alarm/device status for the device. The icon color indicates the severity of the most severe alarm on the device. A red icon indicates a critical alarm or the device is down. A green icon indicates that there are no alarms and the device is up.
- Sparkline Graphs — Provides network trends in dense, succinct charts that present report data in an easy to read, condensed format. You must have Historical Statistic Collection enabled in order to see the Sparkline graphs and other report data. If Historical Statistic Collection is not enabled, you will see a line that says, "Historical Statistic Collection Disabled." For information on configuring data collection, see Collect Device Statistics in the Devices section of the Extreme Management Center User Guide.
- Firmware Updates Available — If there are new firmware releases available for the device (based on the results from the latest Check for Firmware Updates operation), the Firmware Update icon displays. Right-click on the icon to open a window listing the current available firmware releases with links to download the firmware.

- **Device Details Menu** — Click the **Menu** icon (☰) in the upper right corner to access additional device reports.

Launching DeviceView

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

Network Tab

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

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

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

Control Tab

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

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

Extreme Management Center Maps

Use the following steps to launch DeviceView from a map.

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

Search

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

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

Related Information

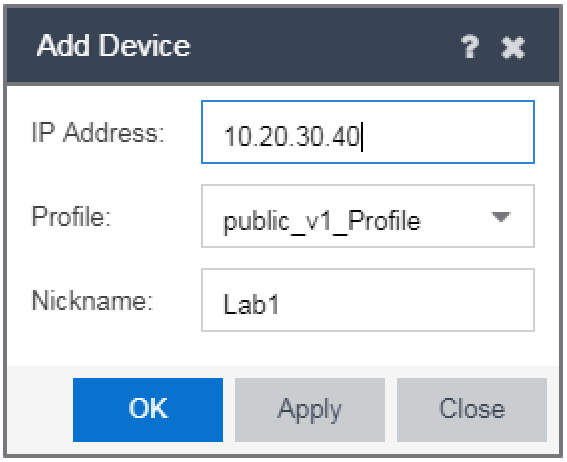
For information on related topics:

- Network Tab

Add Device

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

This window is accessible by clicking the **Menu** icon (≡) and selecting **Device** > **Add Device** from the menu or by right-clicking an existing device and selecting **Device** > **Add Device** on the **Network** > [Devices tab.]



IP Address: 10.20.30.40

Profile: public_v1_Profile

Nickname: Lab1

IP Address

The IP address of the device.

Profile

The access Profile used for the device. To create or edit a profile, open the **Administration** > [Profiles tab].

Nickname

The name by which the device is known.

OK

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

Apply

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

Close

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

Related Information

For information on related windows:

- Discovered

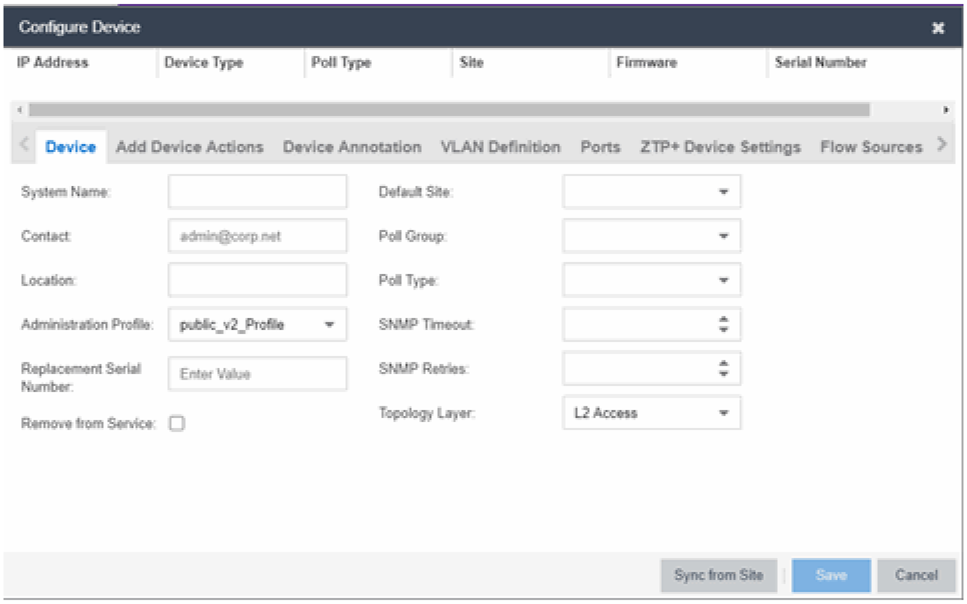
Configure Device

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

To access this window:

1. Open the **Network** > **Devices** tab
2. Select the **Devices** sub-tab.
3. Click the **Menu** icon (≡) or right-click on a device.
4. Select **Device** > **Configure Device**.

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



System Name:

Contact: admin@corp.net

Location:

Administration Profile: public_v2_Profile

Replacement Serial Number: Enter Value

Remove from Service: □

Default Site:

Poll Group:

Poll Type:

SNMP Timeout:

SNMP Retries:

Topology Layer: L2 Access

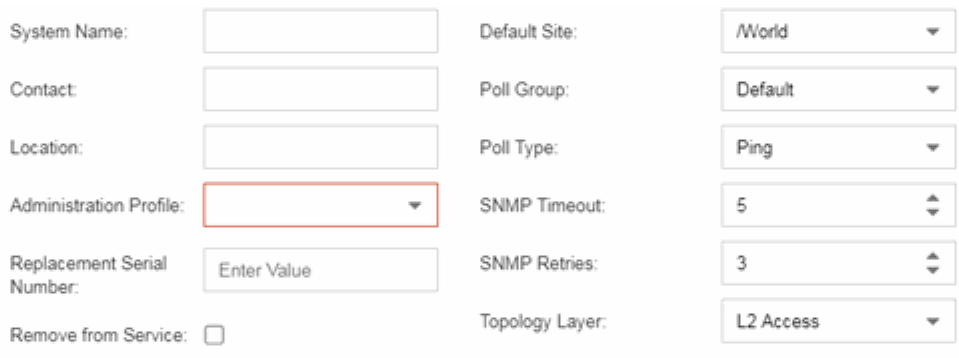
When you first open the window, the **Device** tab opens.

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

- Device
- Device Annotation
- VLAN Definition
- Ports
- ZTP+ Device Settings
- Flow Sources
- Vendor Profile
- Buttons

Device

The **Device** tab displays basic information about the device.



System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	□	Topology Layer:	L2 Access

System Name

The system name of the device. This is displayed in the **Network** > **Devices** tab tree when **Device Tree Name Format** is set to **System Name** in the Local Settings window.

Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "\" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing\John's Devices** in this field.

Location

The physical location of the device. Additionally, enter a backslash "\" between locations to create a device group in a tiered tree structure. For example, to move the device into a device group called "London" within a device group called "Europe", enter **Europe\London** in this field.

Administration Profile

Use the drop-down menu to select the access Profile that gives the Discover tool administrative access to the devices you wish to discover. To create or edit a profile, open the **Administration** > **Profiles** tab.

Replacement Serial Number

Enter the number of the device replacing this device if **Remove from Service** is selected. When entered, Extreme Management Center restores the most recent archive of the device removed from service.

Remove from Service

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

Default Site

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

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center provides three distinct poll groups (configured in the Status Polling view of the **Options** tab) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: If **Poll Type** is **Not Polled** is specified, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

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

- Select **Not Polled** if you do not want to poll the devices.
- Select **Maintenance** if you do not want to poll the devices temporarily. Using this **Poll Type** allows you to search for devices set to **Maintenance** to change them back to their regular **Poll Type** once maintenance on the device is complete.
- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **Ping** for the **Poll Type** if the **Profile** for the IP Range is also set to **Ping**.

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

SNMP Timeout

The amount of time that Extreme Management Center waits before re-trying to contact the device. The value for this setting must be between 3 and 60 seconds.

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

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

SNMP Retries

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

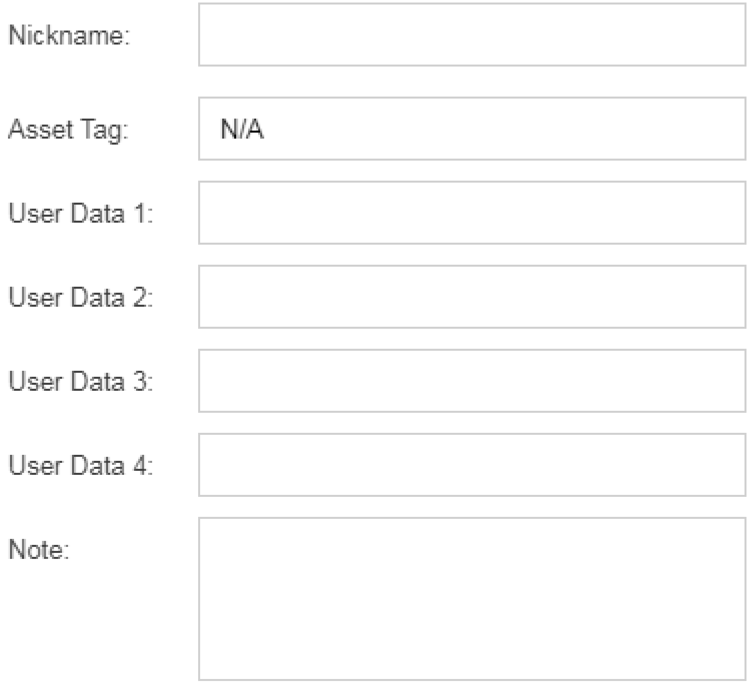
The value entered in this field overrides the default entered in the SNMP Advanced view in the Administration > Options tab.

Topology Layer

The layer and networking attributes for the device.

Device Annotation

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



Nickname:	
Asset Tag:	N/A
User Data 1:	
User Data 2:	
User Data 3:	
User Data 4:	
Note:	

Nickname

The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when Nickname is selected in the

How to Display Devices in Tree menu option in the Extreme Management Center options menu in the Administration > Options tab.

Asset Tag

A unique asset number assigned to a device for inventory tracking purposes.

User Data

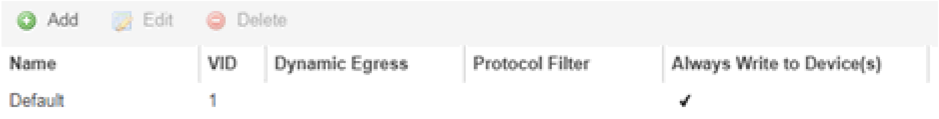
The user-defined information displayed in the devices table in the User Data columns. Additionally, enter a backslash "\" between user data to create a device group in a tiered tree structure. For example, to move the device into a device group called "Dorm 1" within a device group called "Campus", enter Campus\Dorm 1 in this field.

Notes

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

VLAN Definition

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



Name	VID	Dynamic Egress	Protocol Filter	Always Write to Device(s)
Default	1			✓

Name

Displays the name of the VLAN.

VID

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

Dynamic Egress

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

Protocol Filter

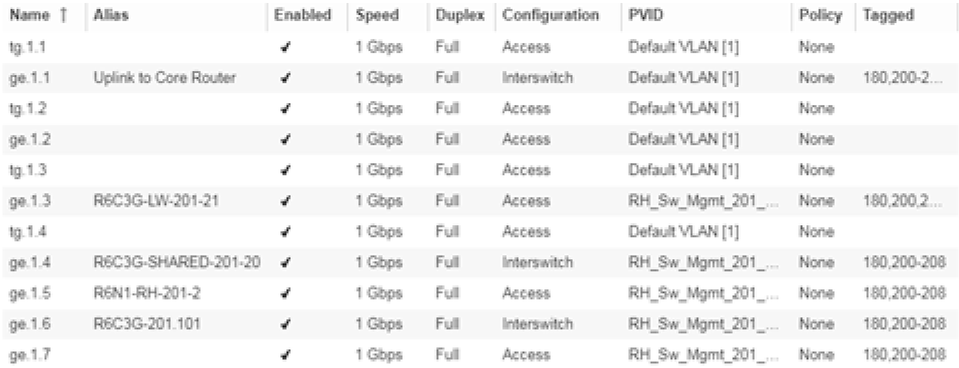
Indicates the VLAN uses an X-Pedition Protocol Filter.

Always Write to Device(s)

Indicates if the VLAN is written to the device whether or not it is being used in a rule or role.

Ports

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



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

Name

Enter the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

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

Auto Negotiation

Displays whether auto negotiation is enabled or disabled on the port. If Auto Negotiation is enabled, multi-speed selections are enabled.

Speed

Displays the current speed of the selected port. Use the drop-down list to select the speed if auto negotiation is enabled on the port.

Duplex

Displays the current duplex mode for the selected port. Use the drop-down list to select the mode if auto negotiation is enabled on the port.

Configuration

Use the drop-down menu to determine the purpose of the port:

- Access — Select this option if the port connects to user end-systems.
- Interswitch — You can also manually select this option if the port is used to connect to other switches. This option is selected by default if the port detects neighboring switches are configurable.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.
- AP — Select this option if the port is used to connect with a networking device that allows a Wi-Fi device to connect to a wired network.
- Phone — Select this option if the port is used to connect to a telephone.
- Router — Select this option if the port is used to connect to a router.
- Printer — Select this option if the port is used to connect to a printer.
- Security — Select this option if the port is used to connect to a device or devices that have been configured with security or advanced security settings.
- IoT — Select this option if the port is used to connect to an additional wireless"smart" device.
- Other — Select this option if the port is used to connect to any other device.

PVID

Select the port's VLAN ID.

LAG

Select to indicate whether the port is part of an active link aggregation group (LAG).

Authentication

Use the drop-down menu to determine whether authentication is required to access the port:

- None — No authentication is required to access the port.
- 802.1X — Select this option to require 802.1X authentication to access the port.
- MAC Auth — Select this option to require authentication based on the users MAC address.

Policy

The policy assigned to the selected port.

Tagged

Select to indicate the port's egress state is tagged.

Untagged

Select to indicate the port's egress state is untagged.

Node Alias

Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard

Select to enable Span Guard, which allows Extreme Management Center to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect

Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point -to -point interswitch links.

- If the ports receive the BPDUs, the link's State becomes Forwarding.
- If a BPDU timeout occurs on the ports, its state becomes listening until a BPDU is received.

MVRP

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

Update

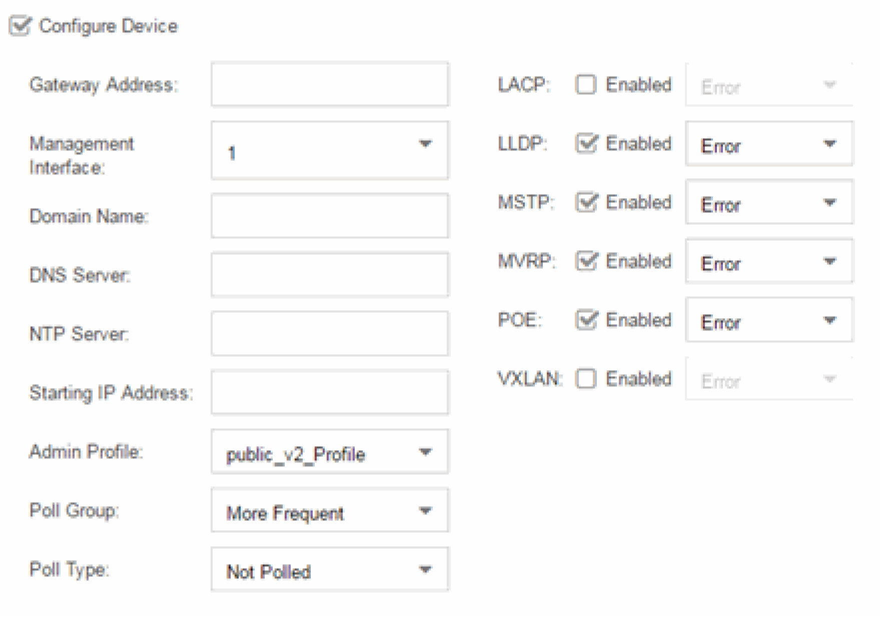
Click Update to save any changes made to the device configuration.

Cancel

Click Cancel to close the window and discard any changes.

ZTP+ Device Settings

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



☑ Configure Device

Gateway Address:		LACP:	☐ Enabled	Error
Management Interface:	1	LLDP:	☑ Enabled	Error
Domain Name:		MSTP:	☑ Enabled	Error
DNS Server:		MVRP:	☑ Enabled	Error
NTP Server:		POE:	☑ Enabled	Error
Starting IP Address:		VXLAN:	☐ Enabled	Error
Admin Profile:	public_v2_Profile			
Poll Group:	More Frequent			
Poll Type:	Not Polled			

Configure Device

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

Gateway Address

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

Management Interface

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

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices being discovered.

DNS Server

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

NTP Server

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

Starting IP Address

The **Starting IP Address** field allows you to set the starting IP address of the IP address range for the ZTP+ devices being discovered.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center administrative access to the ZTP+ devices you wish to discover. Use the Profiles list in the Discover section of the **Site** tab to create or edit a profile. If you discover an existing device using a different profile than the device is already using in the database, saving the device overwrites the profile currently being used in the database.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center provides three distinct poll groups (defined in the Status Polling options (**Administration** > **Options**) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

NOTE: If you select **Not Polled**, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

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

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

LACP

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

LLDP

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

MSTP

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

MVRP

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

POE

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

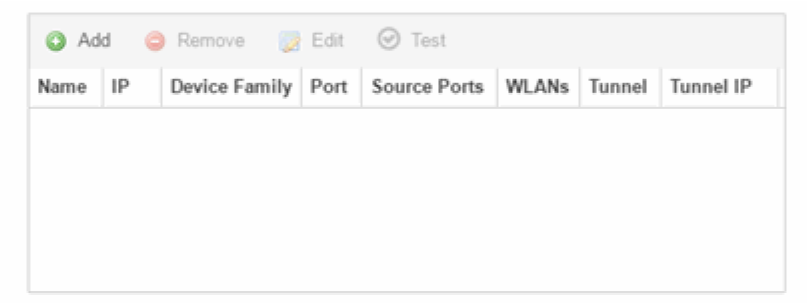
VXLAN

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

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

Flow Sources

The **Flow Sources** tab allows you to configure devices to act as flow sources for a Application Analytics engine.



Name	IP	Device Family	Port	Source Ports	WLANs	Tunnel	Tunnel IP

Name

Displays the name of the flow source device.

IP

Displays the IP address of the flow source device.

Device Family

Displays the device family of the flow source device.

Port

Indicates the mirror port attached to the Application Analytics engine or used to create the GRE tunnel.

Source Ports

Displays the ports on which flow collection is enabled.

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

WLANs

Displays the WLANs of which the wireless controller being used as a flow source device is a member.

Tunnel

Indicates the device is configured to mirror flows using a GRE tunnel.

NOTE: If Tunnel is disabled, the Application Analytics engine must be directly attached to the flow source.

Tunnel IP

Displays the management IP address of the flow source device or the IP address of the loop-back interface on the device.

Add

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

Remove

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

Edit

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

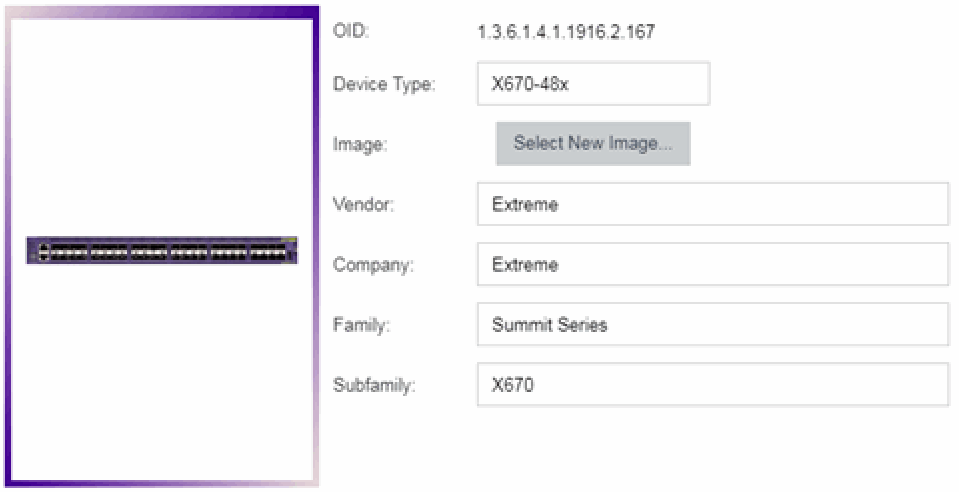
Test

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

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

Vendor Profile

The **Vendor Profile** tab allows you to edit configurations for devices. The configuration you select determines the reports available for the device in its DeviceView and lets you choose the FlexView filters that apply to the device. You can also enter additional information about the device to help identify it in Extreme Management Center as well as identify the scripts that apply to the device.



OID: 1.3.6.1.4.1.1916.2.167

Device Type: X670-48x

Image:

Vendor: Extreme

Company: Extreme

Family: Summit Series

Subfamily: X670

OID

Displays the Object Identifier for the device.

Device Type

Displays the specific type of device.

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

- The tab is named **New Vendor Profile**.
- You cannot use special characters when creating a new **Device Type**.

Image

Indicates the image file used for the device in the DeviceView and Maps.

Vendor

Displays the vendor who sold the device.

Company

Displays the company that manufactures the device.

Family

Displays the group of devices to which the device belongs, known as the device family in Extreme Management Center.

Subfamily

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

Buttons

Enforce Preview

Click to open the Compare Device Configuration window, from which you can view and compare your current configuration and the proposed new configuration. This window allows you to verify all of the changes you are making to your devices and then enforce those changes to the device. This button displays after making a change that affects the device.

Sync from Site

Click to copy the default configurations for the site to all the selected devices.

Save

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

Cancel

Click to discard any unsaved changes and close the window.

Related Information

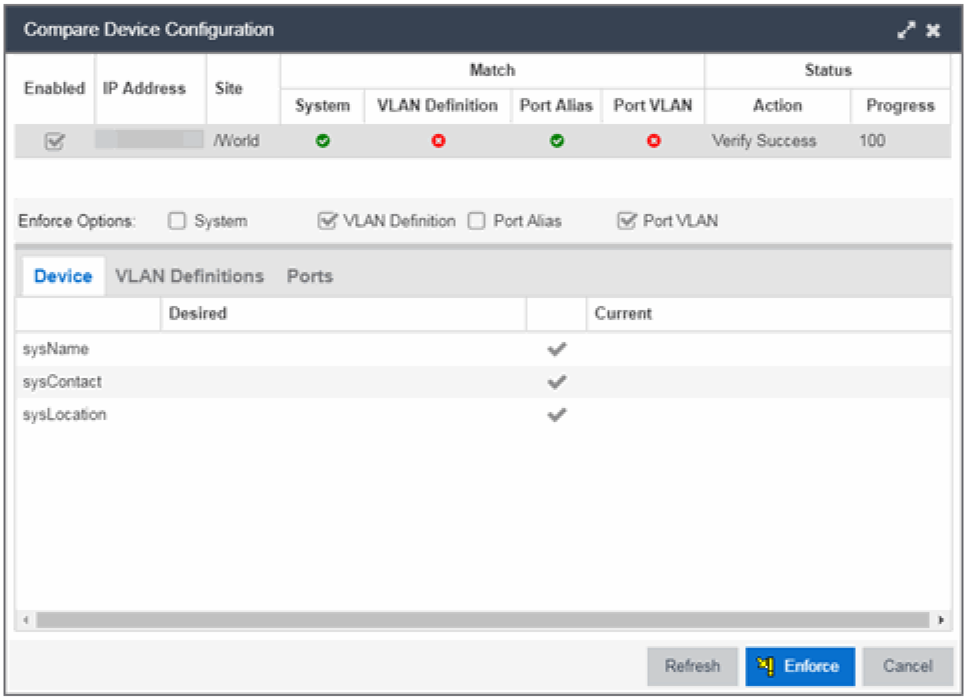
For information on related windows:

- Edit Policy Mapping Configuration Window

Compare Device Configuration

This window allows you to preview changes you make to a device configuration and then enforce them to the device.

To access this window click **Enforce Preview** in the Configure Device window.



Enabled	IP Address	Site	Match				Status	
			System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
☑	[redacted]	/World	✓	✗	✓	✗	Verify Success	100

Enforce Options: □ System ☑ VLAN Definition □ Port Alias ☑ Port VLAN

Device | VLAN Definitions | Ports

	Desired		Current
sysName		✓	
sysContact		✓	
sysLocation		✓	

The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the bottom of the window.

Devices on which the current configuration matches the desired configuration display a check icon (✓), while devices on which differences are detected display a red x (✗). The System column indicates the whether the information on the **Device** tab matches, the VLAN Definition column indicates whether the information on the **VLAN Definitions** tab matches, and the Port Alias and Port VLAN columns indicate whether the information on the **Ports** tab matches.

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

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

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

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

- The Desired column shows the configuration you are saving to the device on the next enforce.
- The Current column shows the configuration currently on the device.

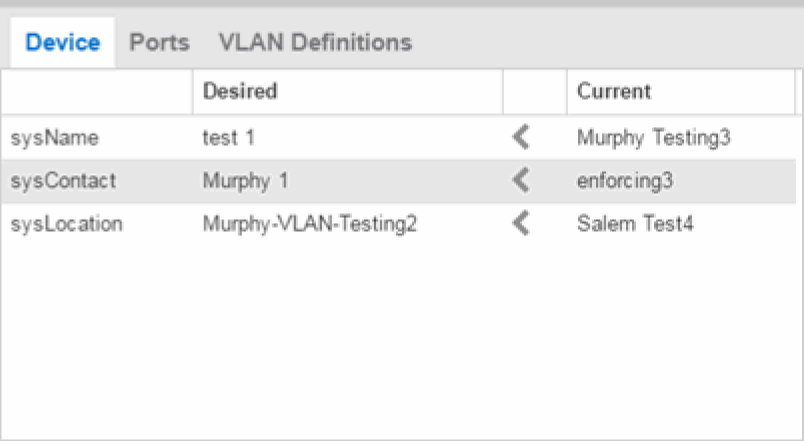
A check mark between the columns (✓) indicates the Current configuration matches the Desired configuration.

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

Click **Enforce** to save your changes to the device.

Device

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



	Desired		Current
sysName	test 1	❮	Murphy Testing3
sysContact	Murphy 1	❮	enforcing3
sysLocation	Murphy-VLAN-Testing2	❮	Salem Test4

sysName

The name by which the device is known.

sysContact

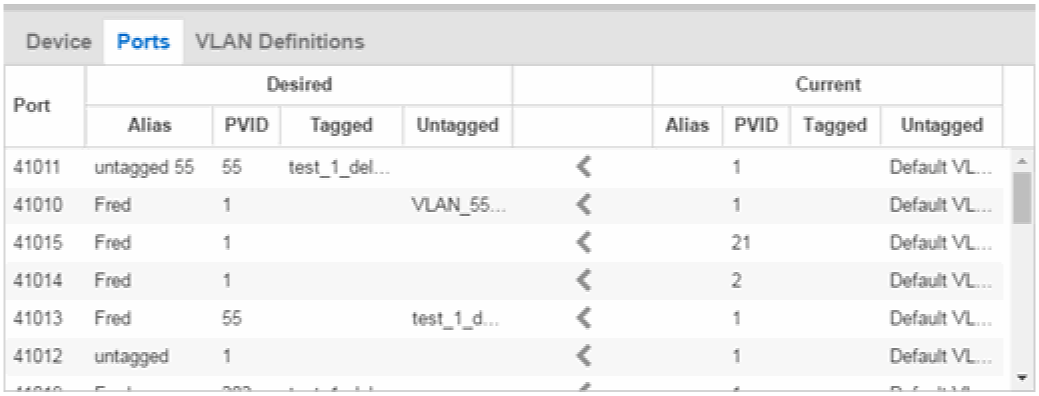
Allows you to specify contact information for the person maintaining the device.

sysLocation

The physical location of the device.

Ports

The **Ports** tab displays any changes to the configuration of ports on the device.



Port	Desired					Current			
	Alias	PVID	Tagged	Untagged		Alias	PVID	Tagged	Untagged
41011	untagged 55	55	test_1_del...		❮		1		Default VL...
41010	Fred	1		VLAN_55...	❮		1		Default VL...
41015	Fred	1			❮		21		Default VL...
41014	Fred	1			❮		2		Default VL...
41013	Fred	55		test_1_d...	❮		1		Default VL...
41012	untagged	1			❮		1		Default VL...

Port

The name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

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

PVID

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

Tagged

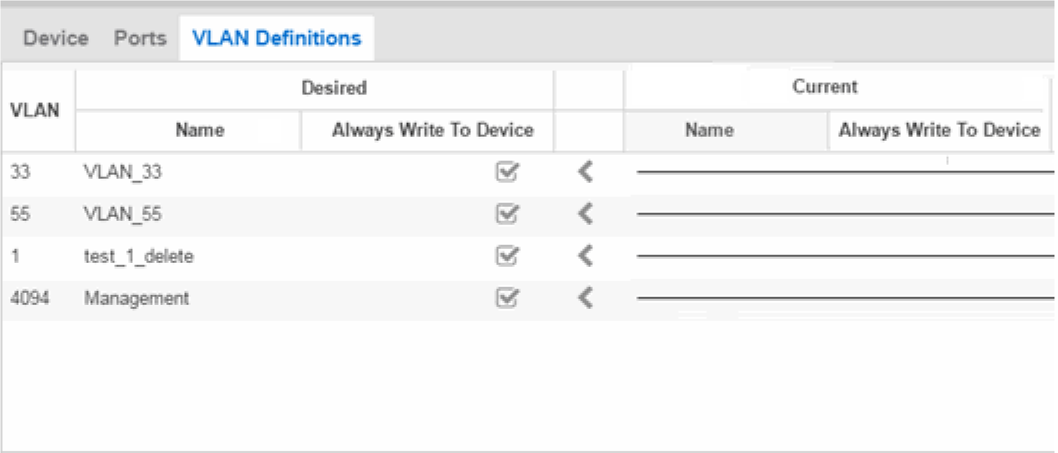
The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged

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

VLAN Definitions

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



VLAN	Desired			Current	
	Name	Always Write To Device		Name	Always Write To Device
33	VLAN_33	☑	<		
55	VLAN_55	☑	<		
1	test_1_delete	☑	<		
4094	Management	☑	<		

VLAN

A unique numerical identifier of the VLAN.

Name

The name of the VLAN.

Always Write to Device(s)

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

Related Information

For information on related topics:

- VLAN Concepts
- Configure Device
- Site Tab

How to Change the Configuration of a Device Included Site

Sites allow you to select the default configuration for devices you add to your network via a device discover or using ZTP+ functionality.

In some instances, a device in a site may need to be configured slightly differently than the other devices in the site.

To change the configuration of a device included in a site:

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down menu.
3. Select the site that includes the device for which you are changing the configuration.
4. In the right-panel, select the **Devices** tab.
5. Right-click the device and select **Device** > **Configure Device**.
   The **Configure Device** window opens.
6. Make the necessary changes and click **Save**.

Related Information

For information on related topics:

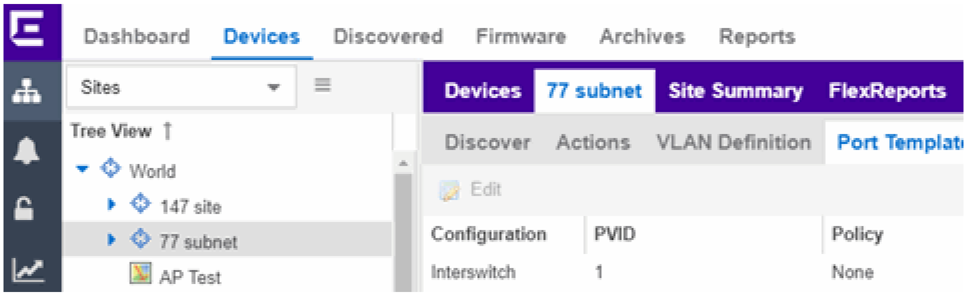
- Sites
- How to Discover Devices in Extreme Management Center
- Devices

Extreme Management Center Site

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

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

Access **Network** > Devices and select **Sites** from the left-panel drop-down menu. Select the site from the left-panel. A tab in the Devices window will open with the name of the site you selected. To create a new site, click the menu icon in the left-panel and select **Maps/Sites** > **Create Site**.



Configuration	PVID	Policy
Interswitch	1	None

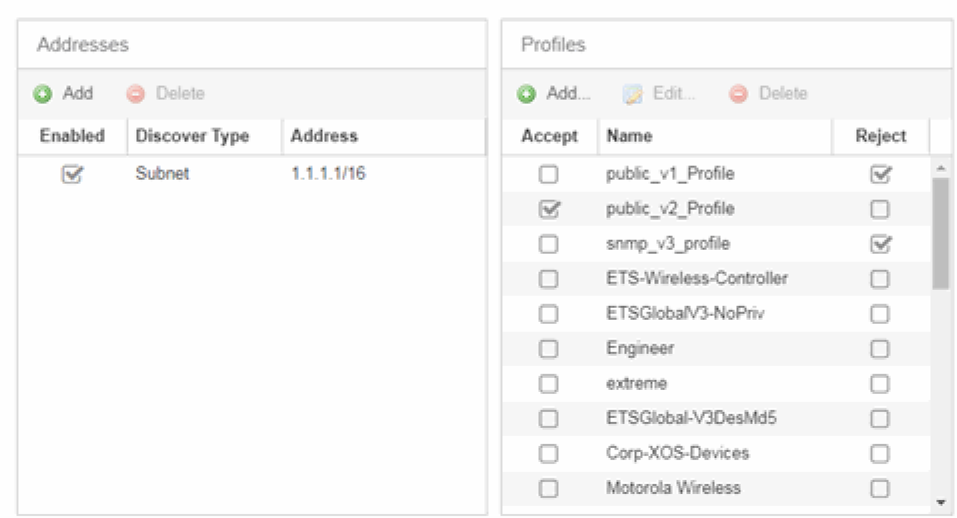
The **Site** tab contains the following tabs:

- Discover
- Actions
- VLAN Definition
- Port Templates
- ZTP+ Device Defaults
- Buttons

Discover

The **Discover** tab allows you to enter address information for new devices on your network, which adds them to the Extreme Management Center database in the current Site. You can perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices, an LLDP (Link Layer Discovery Protocol) discover for LLDP-compliant devices, and an EDP (Extreme Discovery Protocol) discover for EDP-compliant devices. Additionally, you can discover new devices based on subnets or IP address ranges. When discovering devices, you can choose to accept or reject devices based on the profile type using the respective checkboxes in the Profiles section.

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



Enabled	Discover Type	Address
☑	Subnet	1.1.1.1/16

Accept	Name	Reject
□	public_v1_Profile	☑
☑	public_v2_Profile	□
□	snmp_v3_profile	☑
□	ETS-Wireless-Controller	□
□	ETSGlobalV3-NoPriv	□
□	Engineer	□
□	extreme	□
□	ETSGlobal-V3DesMd5	□
□	Corp-XOS-Devices	□
□	Motorola Wireless	□

Addresses

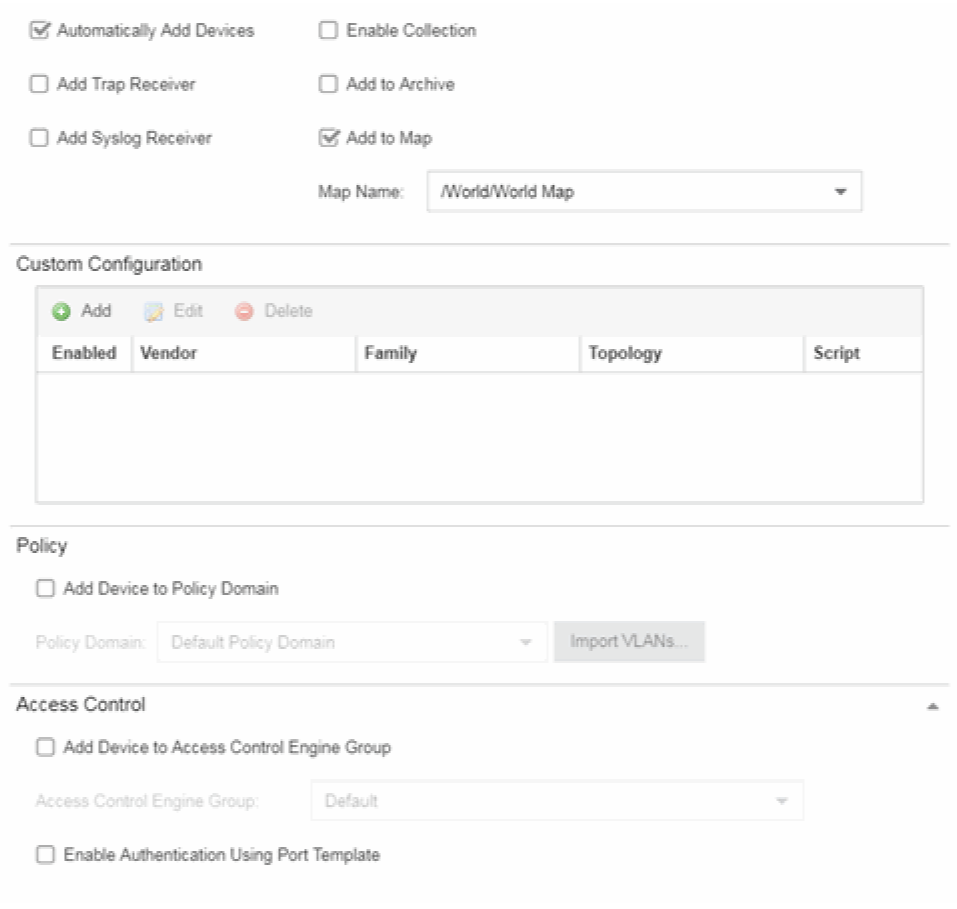
Click the **Add** button in the Addresses list to allow you to add devices by seed address, subnet, or address range. Selecting **Seed Address** allows you to perform a discover for CDP, LLDP, or EDP-compliant devices. Click the **Discover** button at the bottom of the tab to begin the device discover.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

Profiles

Select the access Profiles that gives the Discover tool read access to the devices you wish to discover by selecting the **Accept** checkbox. Select the Profiles that are not valid on the device being discovered by selecting the **Reject** checkbox. To create a profile, click the Add button or edit a profile by clicking the Edit button. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the profile currently being used in the database.

Actions

The **Actions** tab contains basic information about the device being discovered.



☑ Automatically Add Devices

☐ Enable Collection

☐ Add Trap Receiver

☐ Add to Archive

☐ Add Syslog Receiver

☑ Add to Map

Map Name: /World/World Map

Custom Configuration

Enabled	Vendor	Family	Topology	Script

Policy

☐ Add Device to Policy Domain

Policy Domain: Default Policy Domain

Access Control

☐ Add Device to Access Control Engine Group

Access Control Engine Group: Default

☐ Enable Authentication Using Port Template

Automatically Add Devices

Selecting the **Automatically Add Devices** checkbox causes Extreme Management Center to automatically add devices to the database that match the address information you entered in the Discover section of the tab. When this box is NOT selected and a discover occurs, devices are added to the **Network** > **Discovered** tab, where they can be configured prior to being added to the database.

Add Trap Receiver

Select this checkbox to configure devices added to the site to send trap information to Extreme Management Center. You can define the trap configuration details on the **Options** > Trap tab. Depending on the device, Extreme Management Center creates the trap configuration via SNMP or a script.

Add Syslog Receiver

Select this checkbox to configure the devices added to the site to send syslog information to Extreme Management Center. You can define the syslog configuration details on the **Options** > Syslog tab. Depending on the device, Extreme Management Center creates the syslog configuration via SNMP or a script.

Enable Collection

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

Add to Archive

Select this checkbox to create an archive, which saves the configurations of the devices being discovered in the **Network** > **Archives** tab.

Add to Map

Select this checkbox to add the devices being discovered in the site to a map. To add a device to multiple maps, add it via this drop-down menu and then manually add it via the **Maps** > **Add to Map** on the **Devices** tab.

Custom Configuration

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

Policy

Add Device to Policy Domain

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

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

Extreme Access Control

Add Device to Extreme Access Control Engine Group

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

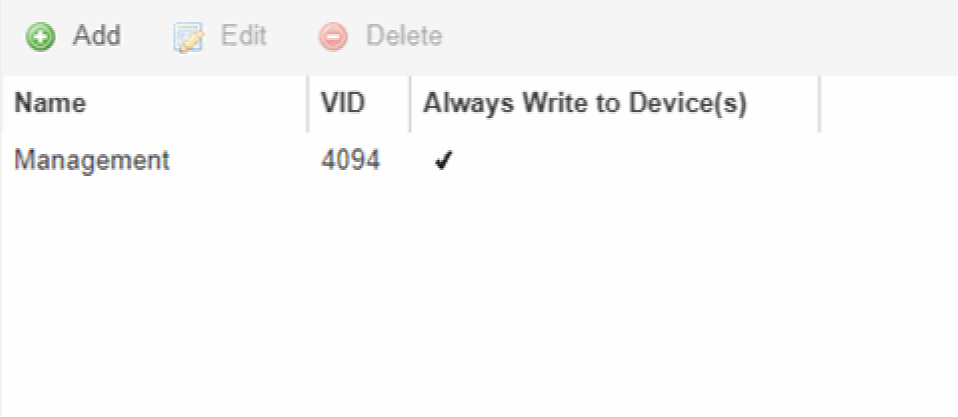
- If the device is an Extreme Access Control engine, it is added as an engine to the engine group.
- If the device is not an engine, it is added as a switch to up to two engines in the engine group. An enforce is run against the engine group if a switch is added.

Enable Authentication Using Port Template

Select this checkbox to allow users to authenticate to the device using a port template. Configure Port Templates in the Port Templates section of the tab.

VLAN Definition

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



Name	VID	Always Write to Device(s)
Management	4094	✓

Name

Displays the name of the VLAN.

VID

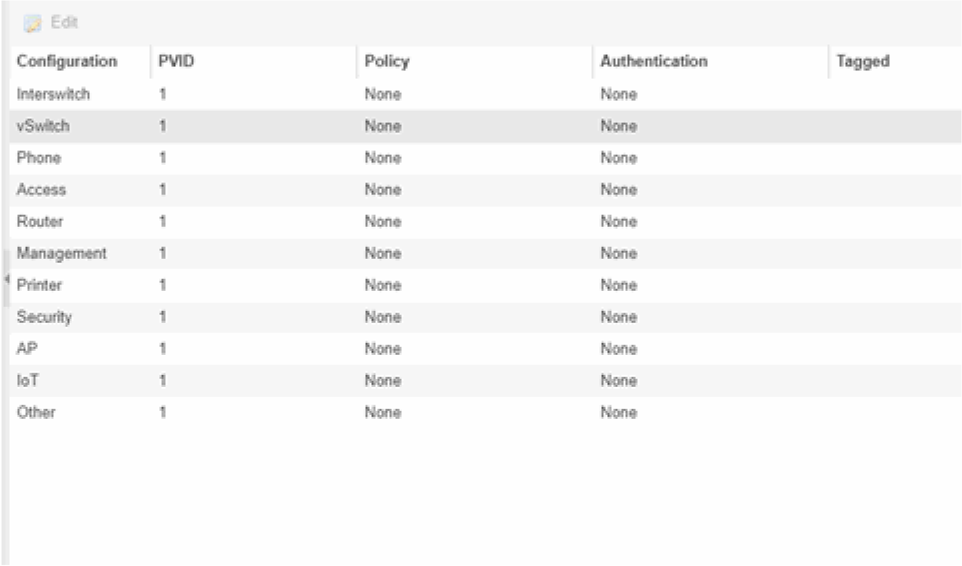
Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Always Write to Device(s)

Indicates if the VLAN is written to the device whether or not it is being used in a rule or role.

Port Templates

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



Configuration	PVID	Policy	Authentication	Tagged
Interswitch	1	None	None	
vSwitch	1	None	None	
Phone	1	None	None	
Access	1	None	None	
Router	1	None	None	
Management	1	None	None	
Printer	1	None	None	
Security	1	None	None	
AP	1	None	None	
IoT	1	None	None	
Other	1	None	None	

Edit

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

Configuration

Use the drop-down menu to determine the purpose of the port:

- **Access** — Select this option if the port connects to user end-systems.
- **Interswitch** — You can also manually select this option if the port is used to connect to other switches. This option is selected by default if the port detects neighboring switches are configurable.
- **Management** — Select this option if the port is used to manage network traffic with Extreme Management Center.
- **AP** — Select this option if the port is used to connect with a networking device that allows a Wi-Fi device to connect to a wired network.
- **Phone** — Select this option if the port is used to connect to a telephone.

- Router — Select this option if the port is used to connect to a router.
- Printer — Select this option if the port is used to connect to a printer.
- Security — Select this option if the port is used to connect to a device or devices that have been configured with security or advanced security settings.
- IoT — Select this option if the port is used to connect to an additional wireless"smart" device.
- Other — Select this option if the port is used to connect to any other device.

PVID

The port's VLAN ID.

Policy

The policy assigned to the selected port. To assign policy to the selected port, select Add Device to Policy Domain and select a Policy Domain from the drop-down menu in the Discovered Device Actions section of the tab. Policy assignment to the port is performed after a successful policy domain enforce.

Authentication

Use the drop-down menu to determine whether authentication is configured to the port:

- None — No authentication is required to access the port.
- 802.1X — Select this option to enable 802.1X authentication to the port.
- MAC Auth — Select this option to enable authentication based on the users MAC address.

WARNING: Configuring the authentication could affect communication to a device and result in loss of connectivity through the interswitch link ports if not detected or configured properly during the discovery process. If you are configuring the policy and authentication on the interswitch link, it's strongly recommended to ensure neighbor discovery protocols such as LLDP, EDP, and CDP are enabled before enabling the authentication using port templates.

Tagged

Indicates the port's egress state is tagged.

Untagged

Indicates the port's egress state is untagged.

Node Alias

Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard

Select to enable Span Guard, which allows Extreme Management Center to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect

Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point -to -point interswitch links.

- If the ports receive the BPDUs, the link's **State** becomes **Forwarding**.
- If a BPDU timeout occurs on the ports, its **State** becomes **Listening** until a BPDU is received.

MVRP

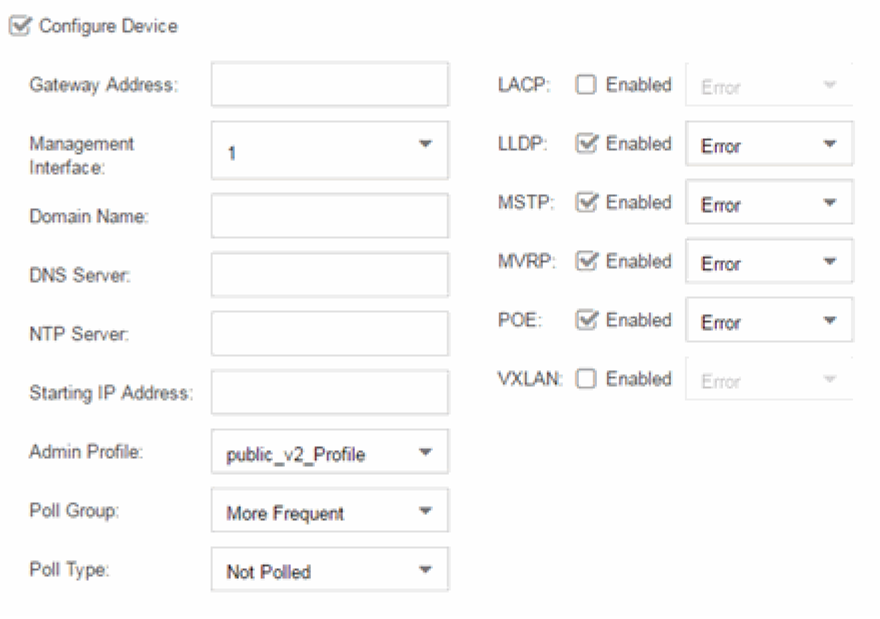
Indicates that the Multiple VLAN Registration Protocol (MVRP) has been enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN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

Collection

Indicates the port's egress state is untagged.

ZTP+ Device Defaults

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



☑ Configure Device

Gateway Address:

Management Interface: 1

Domain Name:

DNS Server:

NTP Server:

Starting IP Address:

Admin Profile: public_v2_Profile

Poll Group: More Frequent

Poll Type: Not Polled

LACP: □ Enabled Error

LLDP: ☑ Enabled Error

MSTP: ☑ Enabled Error

MVRP: ☑ Enabled Error

POE: ☑ Enabled Error

VXLAN: □ Enabled Error

Configure Device

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

Gateway Address

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

Management Interface

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

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices associated with the site.

DNS Server

The **DNS Server** field allows you to set the DNS server address on the ZTP+ devices associated with the site.

NTP Server

The **NTP Server** field allows you to set the NTP server address on the ZTP+ devices associated with the site.

Starting IP Address

The **Starting IP Address** field allows you to set the starting IP address of the IP address range for the ZTP+ devices associated with the site.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center administrative access to the ZTP+ devices associated with the site. Use the Profiles list in the Discover section of the **Site** tab to create or edit a profile. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the device profile currently being used in the database.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center provides three distinct poll groups (defined in the Status Polling options (**Administration** > **Options**) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

NOTE: If you select **Not Polled**, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

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

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

LACP

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

LLDP

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

MSTP

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

MVRP

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

POE

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

VXLAN

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

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

Buttons

Edit Devices

Clicking **Configure Devices** opens the [Configure Device window] for all of the devices added to the site. This allows you to change the configuration of a single device or a subset of devices within the site.

Save

Clicking **Save** saves any changes you make to a site. This button displays after making a change to the tab.

Cancel

Clicking **Cancel** discards any changes you make to a site. This button displays after making a change to the tab.

Discover

Clicking **Discover** adds to the site any new devices that match the criteria entered in the Discover section of the window. This button displays after clicking **Create** or **Save**.

Scheduler

Clicking **Scheduler** opens the **Add Scheduled Task** window, where you can create a new task that automatically adds devices matching the criteria entered in the Discover section of the **Site** tab to the site. This button displays after clicking **Create** or **Save**.

> **NOTE:** After you create a scheduled task to discover devices, edit or delete the task on the Scheduler tab.

Related Information

For information on related topics:

- How to Discover Devices in Extreme Management Center
- Devices
- Maps
- How to Create and Edit Maps
- Advanced Map Features

Compare Device Configurations

You can compare archived device configurations in Extreme Management Center by using either the **Network** > **Devices** tab or the Archive Details Report available in the **Network** > **Reports** tab.

In order to perform the compare configuration operation, you must be a member of an authorization group with the Inventory Manager > Configuration Archive Management > View/Compare Configurations capability.

This Help topic provides the following information:

- Selecting the Files to Compare
- Comparing the Files

Selecting the Files to Compare

Select the files to compare using either the **Network** tab or the **Reports** tab.

From the Network tab:

Use the **Network** tab to compare the last two archived configuration files for a device.

Select a device in the table and use either the **Menu** icon (≡) or the right-click menu off the device to select Configuration/Firmware > Compare Last Configurations.

From the Reports tab:

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

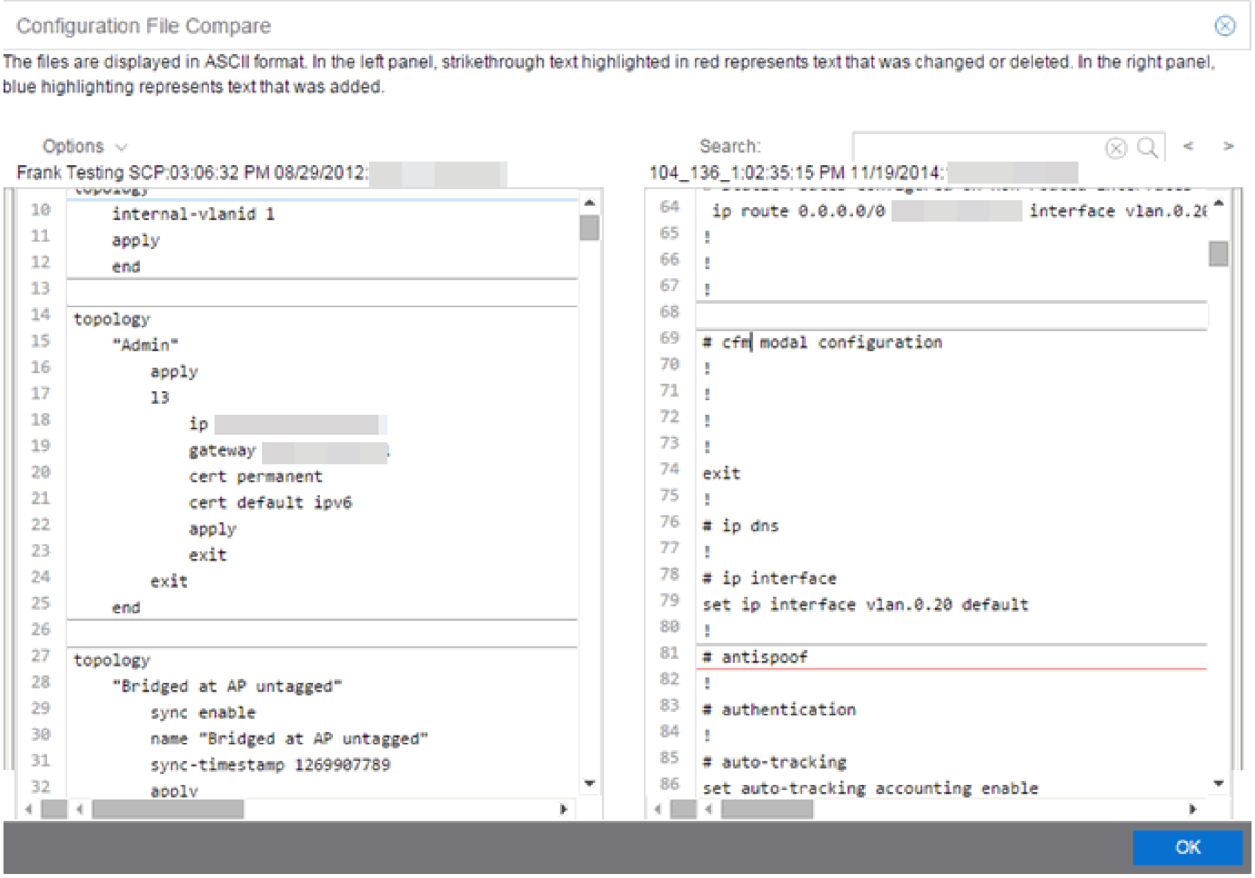
Select the Device > Device Archives report. Click on the **Archive Details** tab in the right panel and then click on the **Archives by Device** sub-tab.

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

Comparing the Files

The Configuration File Compare window displays the files in two panels. Titles over each file show the archive name that contains the configuration file, the date, and the IP address of the device from which you create the configuration file.

Scroll through the two files to view file differences. Typically, the newer file displays in the right panel. You can use the "Swap sides" option to swap the files. In the left panel, strikethrough text highlighted in red represents text that is changed or deleted. In the right panel, blue highlighting represents text that is added.



Configuration File Compare

The files are displayed in ASCII format. In the left panel, strikethrough text highlighted in red represents text that was changed or deleted. In the right panel, blue highlighting represents text that was added.

Frank Testing SCP:03:06:32 PM 08/29/2012:[redacted]

```
topology
    internal-vlanid 1
    apply
    end

topology
    "Admin"
        apply
        l3
            ip [redacted]
            gateway [redacted]
            cert permanent
            cert default ipv6
            apply
            exit
        exit
    end

topology
    "Bridged at AP untagged"
        sync enable
        name "Bridged at AP untagged"
        sync-timestamp 1269907789
        apply
```

104_136_1:02:35:15 PM 11/19/2014:[redacted]

```
 ip route 0.0.0.0/0 [redacted] interface vlan.0.2(
!
!
!

# cfm modal configuration
!
!
!
!
exit
!
# ip dns
!
# ip interface
set ip interface vlan.0.20 default
!
# antispoof
!
# authentication
!
# auto-tracking
set auto-tracking accounting enable
```

Use the toolbar Options menu to control the look of the display window:

- Enable line numbers displays line numbers alongside the text.
- Wrap lines shows all the text in the column and removes the horizontal scroll bars.
- Enable side bars shows where the text differences are in the whole file.
- Swap sides swaps the files contained in the left and right panels.

TIP: Removing line numbers and side bars may speed up the display of larger files.

Use the **Search** field in the toolbar to perform a search in the panel side that is selected by the cursor. Use the forward and back arrows to search for the next or previous instance of the search term.

Related Information

For information on related topics:

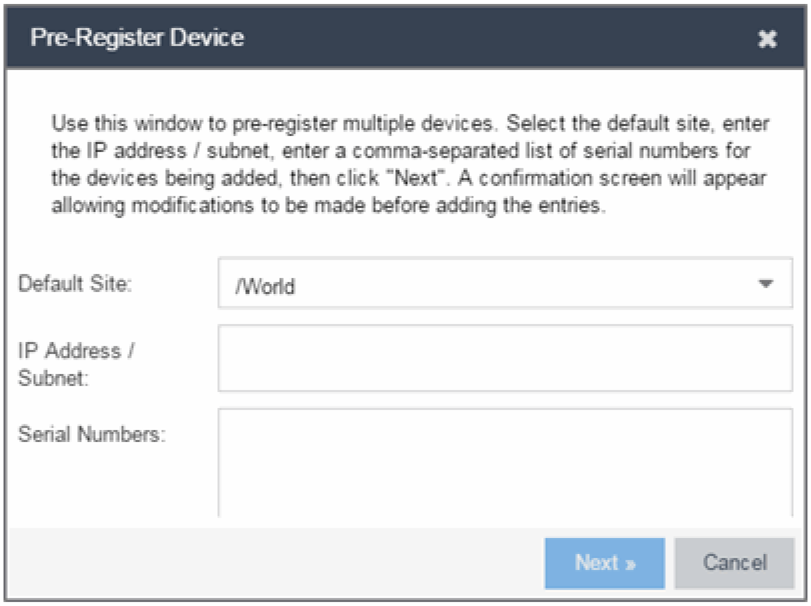
- Network
- Reports

Pre-Register Device

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

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

Pre-Register Device Window



Pre-Register Device

Use this window to pre-register multiple devices. Select the default site, enter the IP address / subnet, enter a comma-separated list of serial numbers for the devices being added, then click "Next". A confirmation screen will appear allowing modifications to be made before adding the entries.

Default Site: /World

IP Address / Subnet:

Serial Numbers:

Default Site

The site to which the devices are added.

IP Address/Subnet

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

Serial Number

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

Next

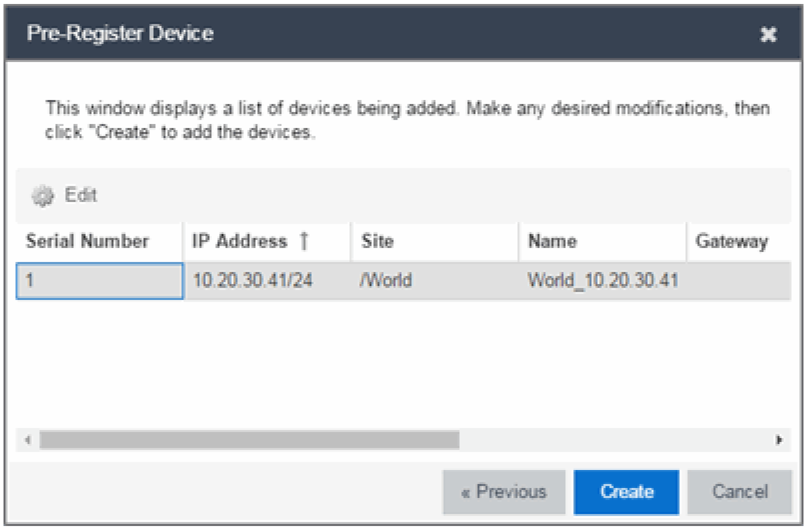
Click the **Next** button to open a confirmation window allowing you to verify the device information entered.

Cancel

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

Pre-Register Device Confirmation Window

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



This window displays a list of devices being added. Make any desired modifications, then click "Create" to add the devices.

Serial Number	IP Address	Site	Name	Gateway
1	10.20.30.41/24	/World	World_10.20.30.41	

Configure

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

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

Serial Number

The serial number of the device.

IP Address

The device's IP address.

Site

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

Name

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

Gateway

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

Domain Name

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

DNS Server

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

NTP Server

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

Create

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

Related Information

For information on related windows:

- Discovered

Maps Overview

The Extreme Management Center Maps feature on the **Network** > **Devices** tab lets you view and search geographic and topology maps of the devices and floor plans of wireless access points (APs) on your network. Use maps to view devices and network connections, device and alarm status; access device and connection information via a right-click menu off the device; and search for devices, APs, and wired or wireless clients.

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

Accessing Maps

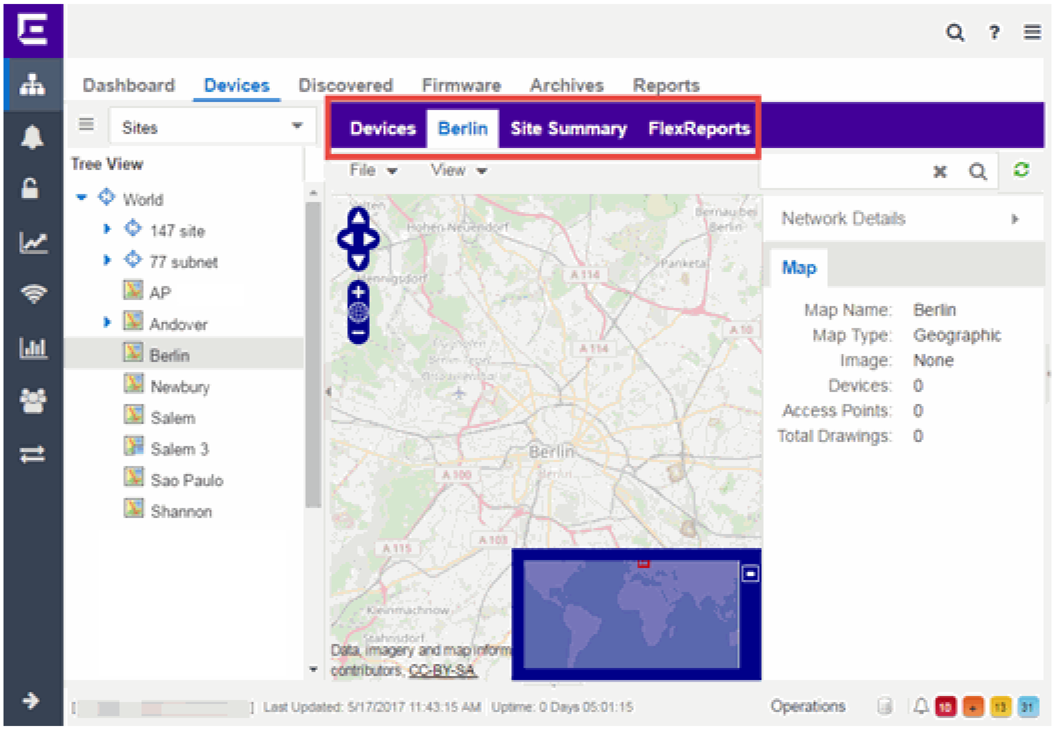
Access the **Network** > **Devices** tab and select **Sites** from the left-panel drop-down menu.

Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

When opening the World map for the first time, the map is blank. As you create maps, add links to them from the World map as shown in the diagram below, allowing you to find individual maps quickly from one map.

Navigating Maps

Selecting a map in the left-panel provides you with tabs at the top of the right-panel that allow you to view information about the devices included in the map:



Map Name: Berlin
Map Type: Geographic
Image: None
Devices: 0
Access Points: 0
Total Drawings: 0

Last Updated: 5/17/2017 11:43:15 AM Uptime: 0 Days 05:01:15

Devices

This tab displays a table of the devices contained within the map. This table is identical to the Devices list available by selecting All Devices in the left-panel drop-down menu, but is filtered to only show the devices added to the map. For additional information about operations available on this tab, see the Devices tab.

Map

This tab, which will show the name of the map you selected from the left-panel, contains the map of the devices. Using Maps, three types of maps are available, Topology, Floorplan, and Geographic. For additional information about operations available on this tab, see the **Map** tab.

For information on creating maps, see How to Create and Edit Maps.

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

Site Summary

The **Site Summary** tab contains a table showing the site paths and configuration information for each site.

FlexReports

This tab contains reports available for the devices included in the site, filtered to display the information selected in the tree (e.g. a site, map, device, controller). Use the drop-down menus to change the report displayed. Each report allows you to configure how the information displays. You can configure Extreme Management Center to automatically create FlexReports on a scheduled basis by clicking the **Schedule** icon, which opens Scheduler. Additionally, FlexReports can be exported in PDF format.

Related Information

For information on related topics:

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

Navigating the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab. This topic shows you how to navigate the Map Tab and its many tools and features.

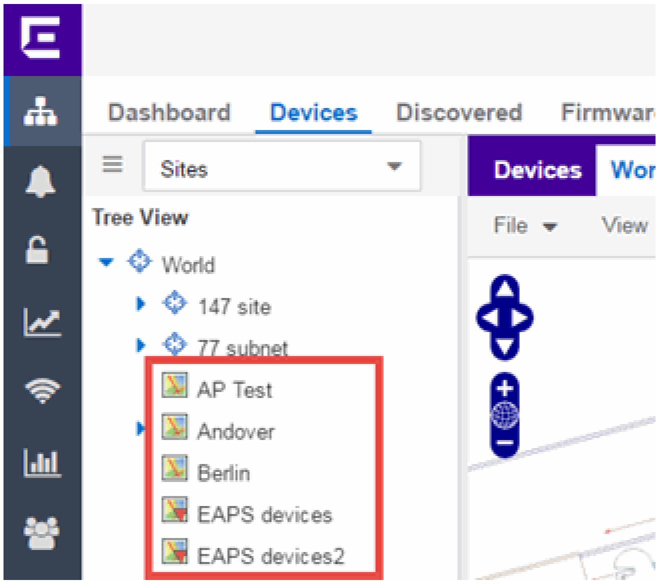
To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

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

World Map Navigation Tree

Select the World Map tree in the left-panel. As you create your maps, they appear in the navigation tree, nested under the map you configure as the **Parent Map**.



As shown in the image above, you also have the ability to nest maps within other maps. This allows you to organize certain maps as a subset of other maps (for example, creating a building map and then creating a map for each of the floors of the building).

Create Map

Right-click a map in the left-panel navigation tree and select **Maps** > **Create New Map** to create a new map. The first map you create is nested under the World Map. All subsequent maps are nested under the map you right-click when creating the new map.

Edit Map

Right-click a map in the navigation tree and select **Maps** > **Edit Map** to open an existing map in edit mode. Edit mode allows you to add new or move existing devices, APs, and map links on a map.

Import Map

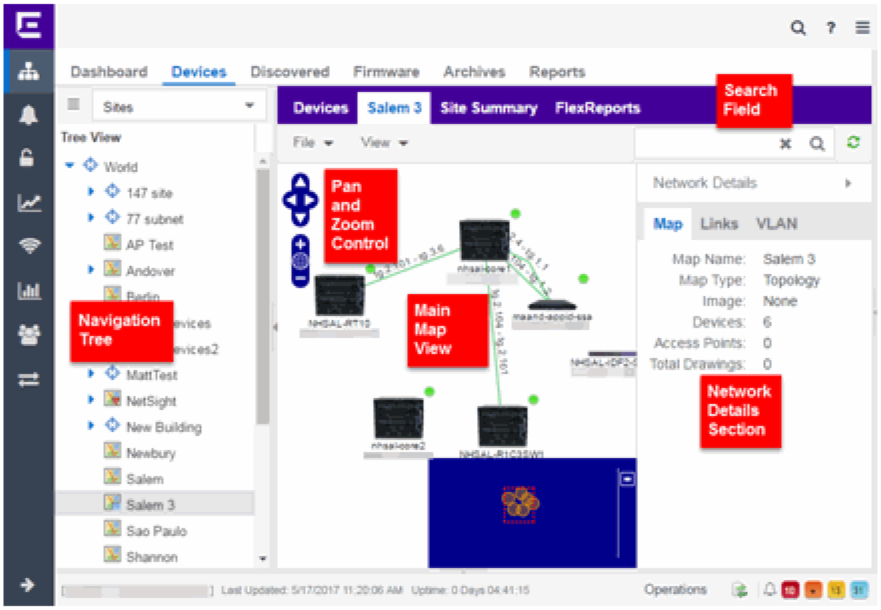
You can also import a saved map by right-clicking a map in the navigation tree and selecting **Maps** > **Import Map**. This opens the Import Map window.

Main Map View

The Main Map view displays your map with all of the devices, network connections, links, or APs, depending on the type of map.

In the Main Map view, you can reorganize the orientation of elements in your map and view the status and details of the elements within the map. The Main Map view also contains the following controls for working with maps:

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

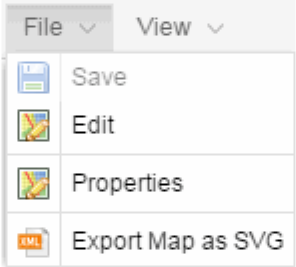


Map Name: Salem 3
Map Type: Topology
Image: None
Devices: 6
Access Points: 0
Total Drawings: 0

File, View, and Tool Menus

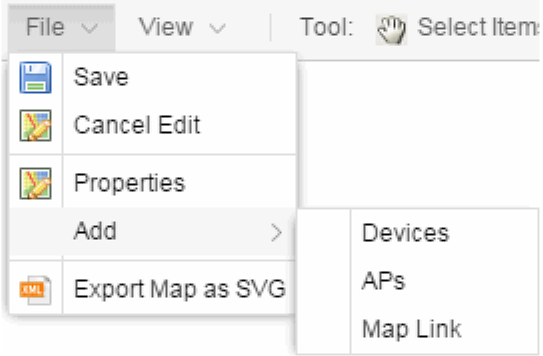
File Menu

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



NOTE: To change the image used for a device type in a map, right-click the device and select Customize Device Type Image. The Upload Custom Device Type Image window appears where you can drag and drop the new image file. The height and width of image files must be less than 1,000 pixels.

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



Clicking **Properties** opens the Map Properties window, which allows you to view and edit information about the map, including the map type, name, and background image. With an NMS-ADV license, the **Export Map as SVG** and **Export Map as ZIP** options are available in the **File** menu, which allow you to export the map in SVG or ZIP format, respectively.

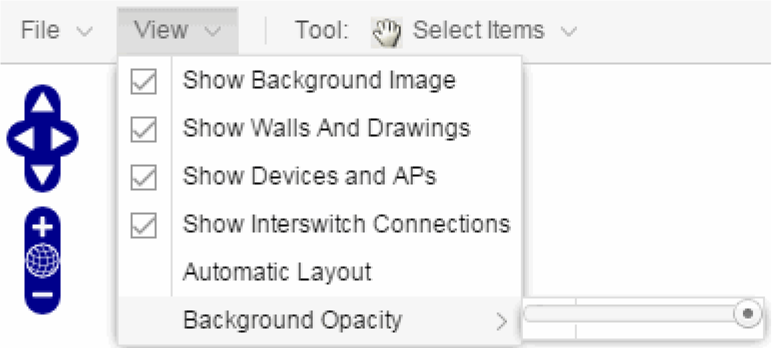
When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated with those devices, your SVG file is identical to the view on your screen; displaying the two devices surrounded by boxes containing the VLAN names. To save the SVG file locally, right-click the map and select **Save as**.

Only floorplan maps can be exported as a ZIP file. Floorplan maps you export as a ZIP file are typically used to import a floorplan into another instance of Extreme Management Center.

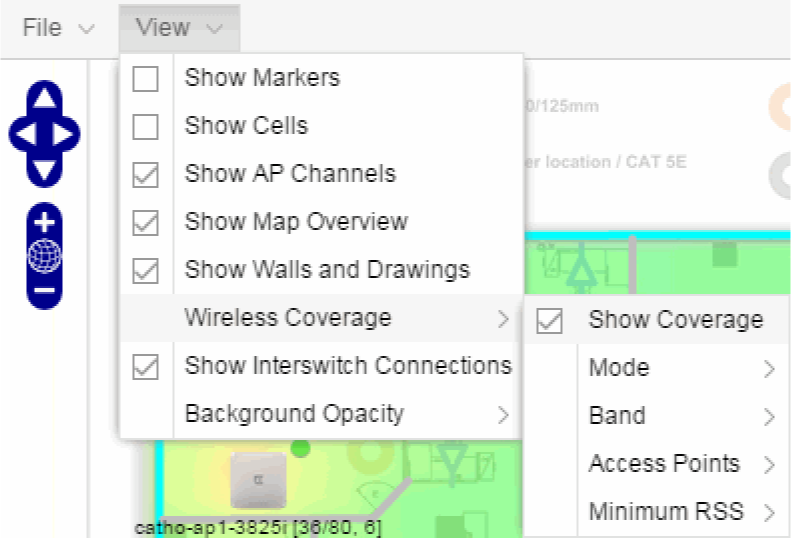
Additionally, by clicking **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Click **Cancel Edit** to exit Edit mode. If you made any changes to the map, a dialog box appears from which you can choose to save the changes or exit Edit mode without saving your changes.

View Menu

The **View** menu allows you to show or hide parts of your map. The options in the **View** menu do not change the information in the map, only allow you to show or hide additional information.



These options vary depending on the map Type. For example, floorplan maps display additional options, including the image you selected as the background of your map, the grid cells that establish the scale of the floorplan, the AP channels for floorplans, the map overview, the walls and drawings of the building, the wireless coverage within a floorplan, the interswitch connections, and the opacity of the background image.



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

Tool Menu

The **Tool** menu allows you to add lines and shapes to your maps. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
✋	Select Items Click on a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Click anywhere on the map and drag to reposition the map image.
⬠	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.
▭	Draw Rectangle Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
✎	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click to add the text to your map. Use the **Style** menu to change the text appearance.
△	Draw Triangle Position the cursor where you want the triangle. Click and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
⌒	Draw Line Position your cursor where you want to start drawing the line. Click once and draw the line. Click to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.

Drawing Tool	Definition
↻	Rotate Shape Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)

Pan and Zoom Control

Pan Control

The **Pan** control allows you to move left/right and up/down in the map. You can also change the position of the map by clicking and dragging the map in any direction.

Zoom Control

The **Zoom** control lets you zoom in and out of the map. You can also zoom in and out of the map by rotating the mouse scroll wheel forward and backward, respectively. Clicking the globe icon in the center of the **Zoom** control resets the zoom and positioning for the map to the last view configured in edit mode.

NOTE: Changing the location and zoom using these controls and then saving the map saves those orientation changes to the map.

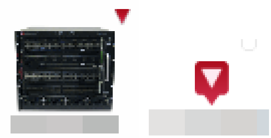
Search Field

Use the **Search** field to search for a wireless client, an AP, or for a device or wired client. Enter a MAC address, IP address, hostname, user name, or AP serial number in the **Search** field and press **Enter** to start a search for a device or wired client.

Clicking the **Refresh** button ⟳ to the right of the **Search** field refreshes the map, including the position of mobile devices connected to an AP. When you click the **Refresh** button, the position of mobile devices updates according to their most recent location.

Viewing Alarm/Device Status

Maps display an integrated alarm/device status either to the right of a device or AP image, or incorporated as part of a map marker (if you have **Show Markers** selected from the map View menu). For example, the device below is down and a critical alarm is triggered (shown as a device image and as a marker).



Alarm status automatically updates every 30 seconds. Change this status refresh interval in the Extreme Management Center options (Administration > Options > OneView > Map).

- ▼ (Red) Critical — There is a critical alarm and the device is down.
- ▶ (Orange) Error — There is a problem with limited implications on the device.
- ▲ (Yellow) Warning — There is a condition that might lead to a problem on the device.
- ■ (Blue) Info — There is an information-only alarm on the device.
- ● (Green) Clear — There are no alarms and the device is up.

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

Accessing Device Information

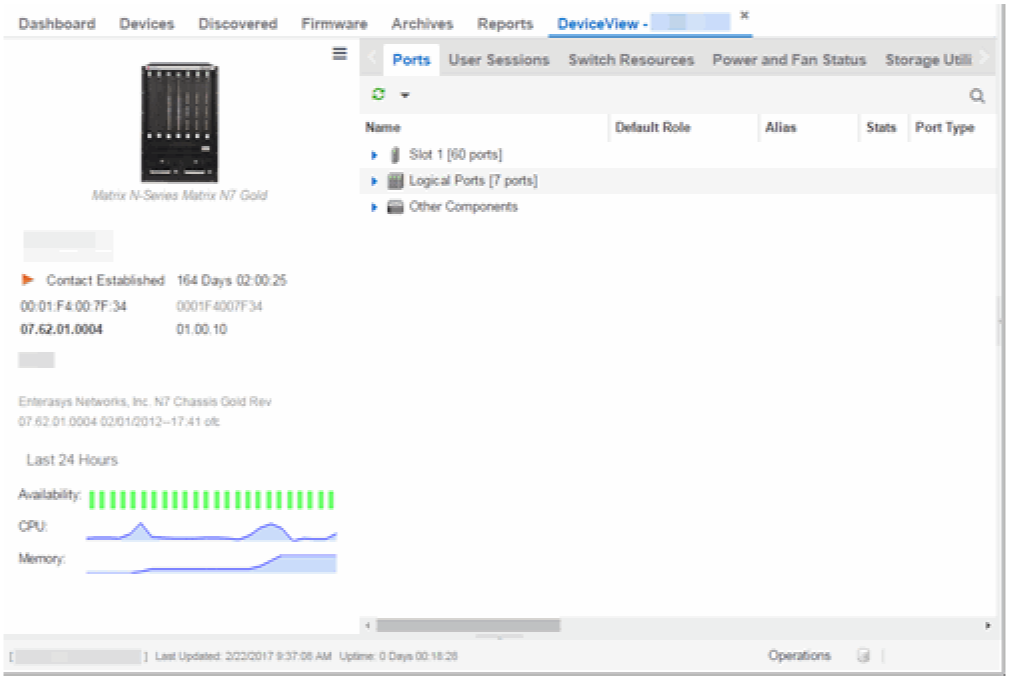
There are two ways to access additional device information from a map.

Device Reports

Launch device information reports from a right-click menu on a device or AP in a map. The menu displays different options based on the device type. You must be in Edit mode to see the **Remove From Map** option.

Device/AP Details

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



Name	Default Role	Alias	Stats	Port Type
Slot 1 [60 ports]				
Logical Ports [7 ports]				
Other Components				

Contact Established 164 Days 02:00:25
00:01:F4:00:7F:34 0001F4007F34
07.62.01.0004 01.00.10

Enterasys Networks, Inc. N7 Chassis Gold Rev 07.62.01.0004 02/01/2012--17:41 ofc

[[redacted]] Last Updated: 2/22/2017 9:37:08 AM Uptime: 0 Days 00:18:28

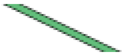
Additionally, the DeviceView and AP PortView windows contain tabs with additional information about the device or AP.

Link Information

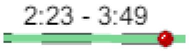
Links are displayed on Topology maps. Each connection type is represented by a different line style:

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

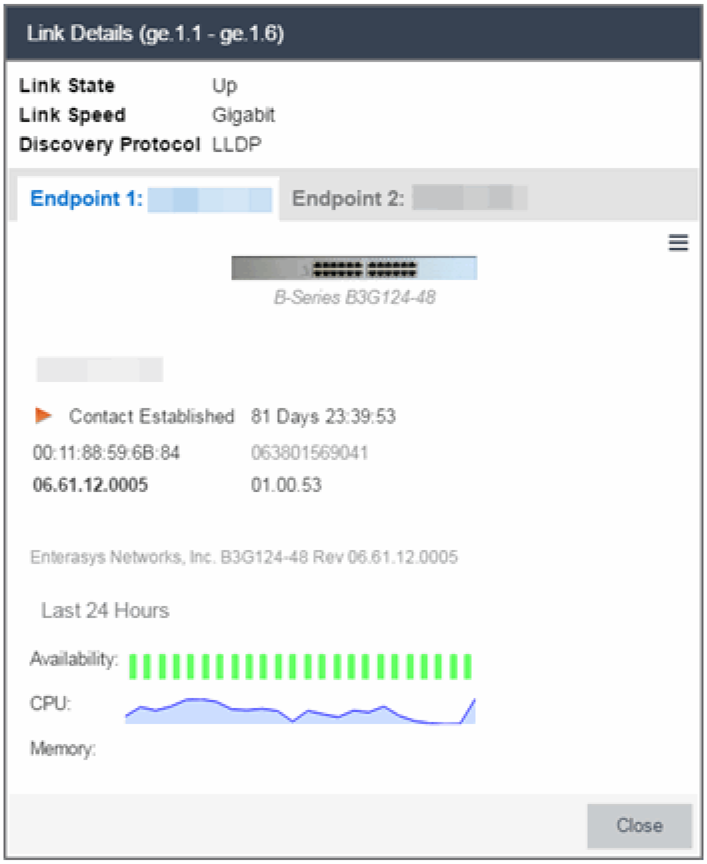
- Shared links appear as basic links when the EAPS domain is not highlighted and appear as thick green lines outlined by a black solid line when you highlight the associated EAPS domain.
- Lag links also appear as thick green lines outlined by a black solid line, but are thicker than shared links and 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.


Link Details (ge.1.1 - ge.1.6)

Link State Up
Link Speed Gigabit
Discovery Protocol LLDP

Endpoint 1: [redacted] Endpoint 2: [redacted]

B-Series B3G124-48

[redacted]

Contact Established 81 Days 23:39:53
00:11:88:59:6B:84 063801569041
06.61.12.0005 01.00.53

Enterasys Networks, Inc. B3G124-48 Rev 06.61.12.0005

Last 24 Hours

Network Details Section

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

- Map tab — Displays information about the map
- EAPS Summary tab — Lists information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature
- Link Summary tab — Displays information about the network connections between devices

- VLAN Summary tab — Lists any virtual local area networks within the map
- MLAG Summary tab — Lists devices configured in a multi-switch link aggregation group
- VPLS Summary tab — Displays information about site connectivity within a private VLAN

Related Information

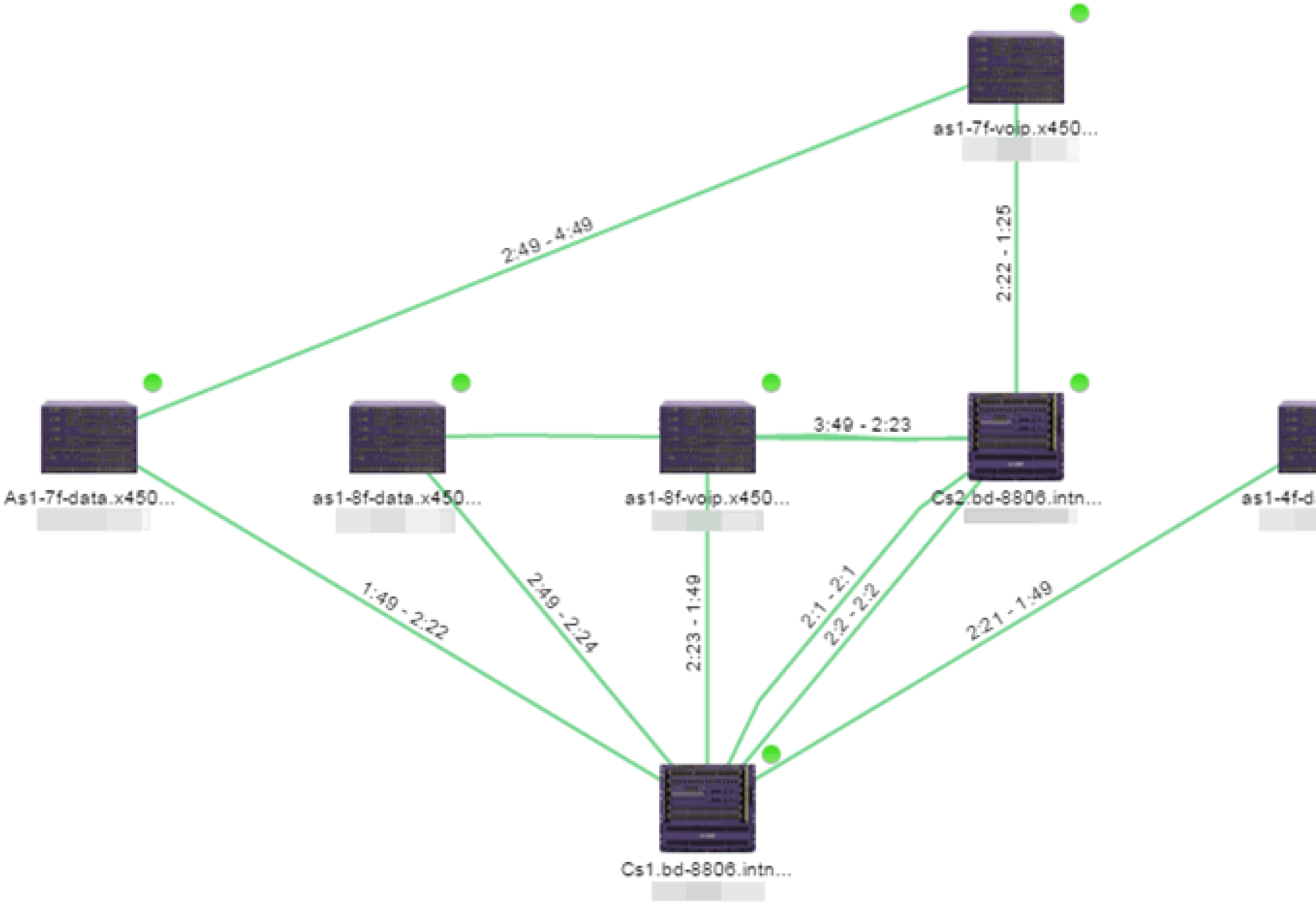
- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center Maps

Extreme Management Center allows you to create geographic and topology maps of devices and floor plans of wireless access points (APs) on your network. Use maps to view devices and network connections, device and alarm status; access device and connection information via a right-click menu off the device; and search for devices, APs, and wired or wireless clients. Maps are configured in various places on the **Network** > **Devices** tab.

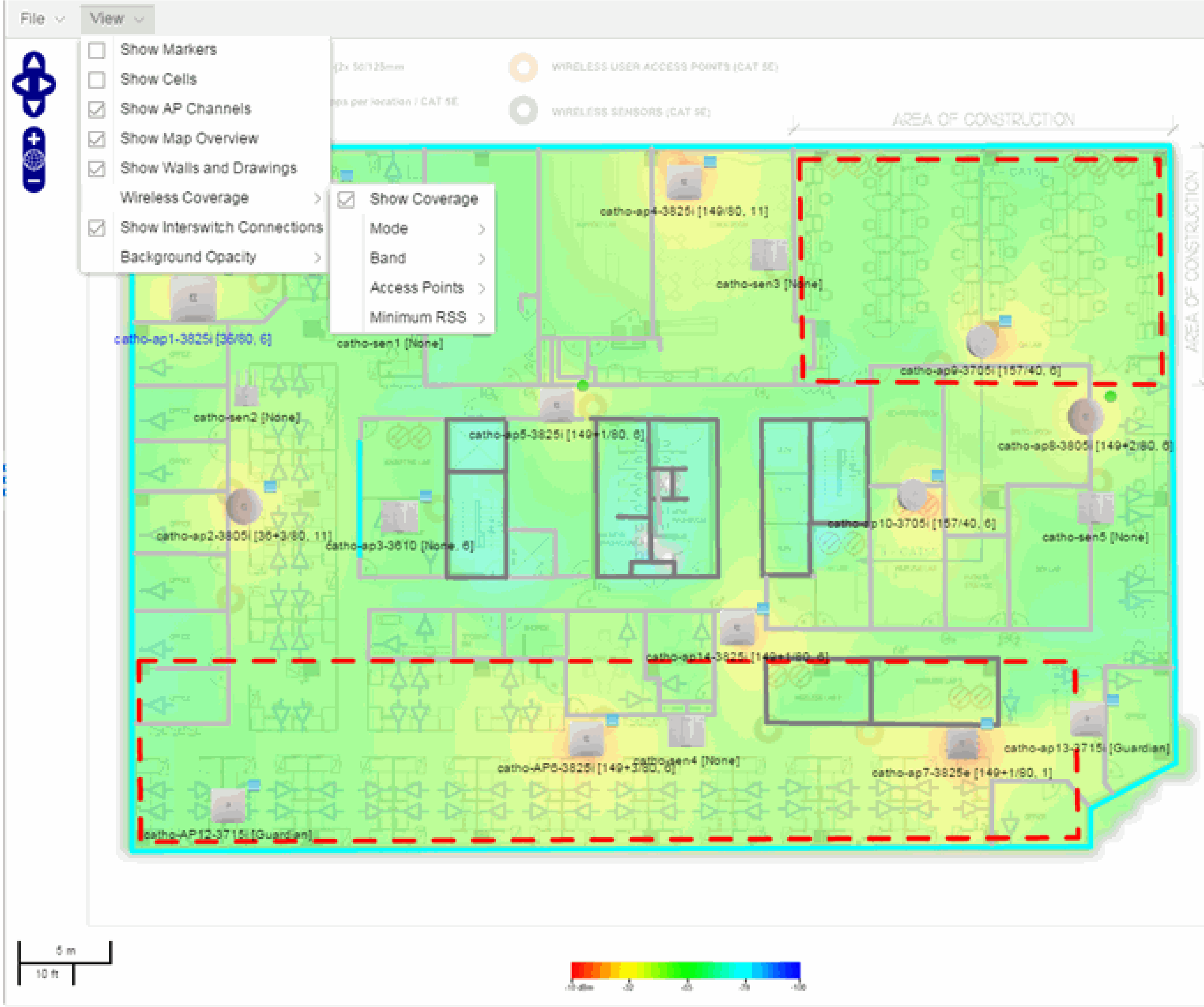
Using Extreme Management Center Maps, you can create three types of maps, each presenting a different visual representation of your network:

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



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

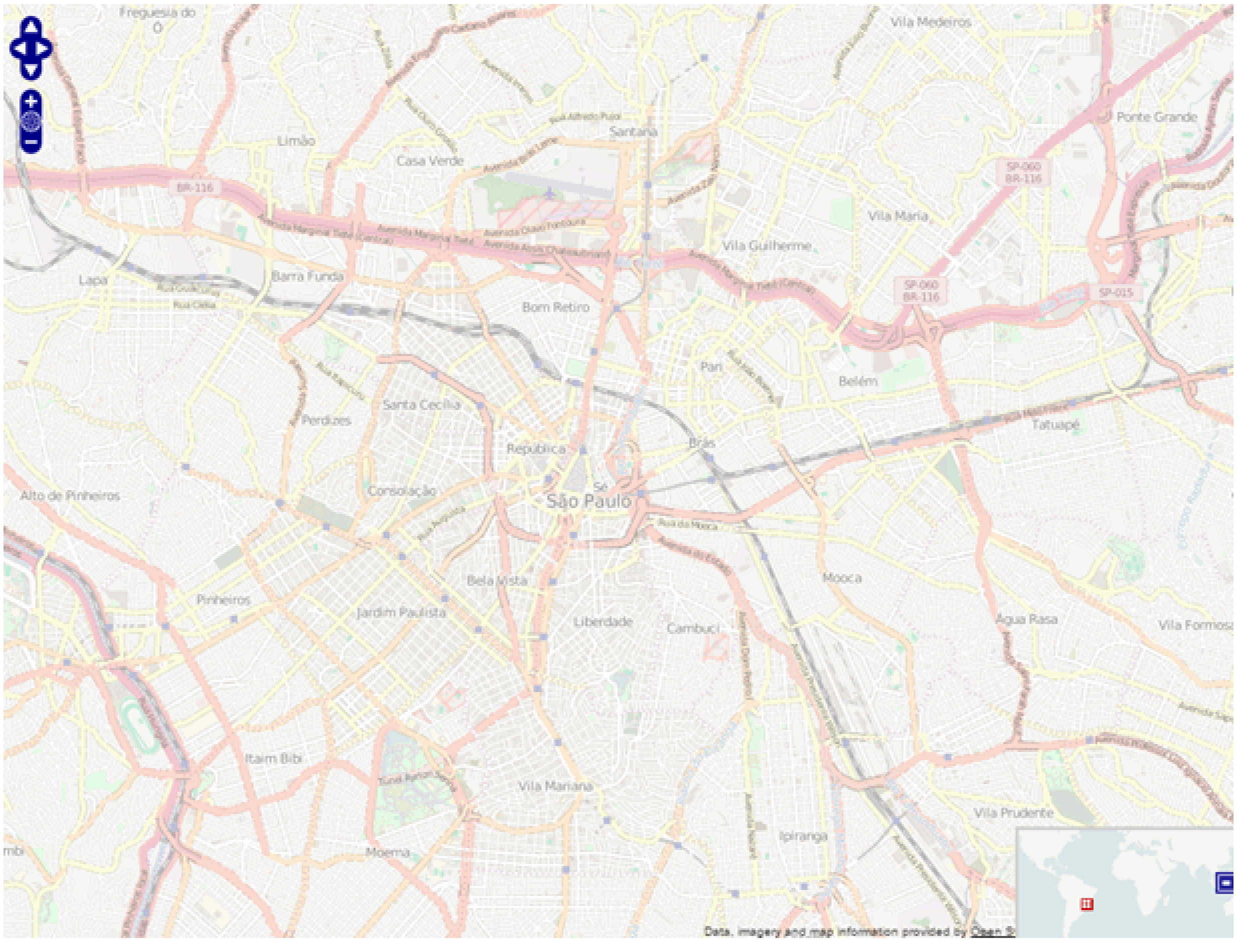
- Floorplan — The floorplan map displays the location of APs in a floorplan you configure. Using information about the size and composition of the building, this map provides an overview of the coverage of wireless APs.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage >
☑ Show Interswitch Connections
Background Opacity >
☑ Show Coverage
Mode >
Band >
Access Points >
Minimum RSS >
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTION
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-3805i [149+2/80, 6]
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-sen5 [None]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap13-3715i [Guardian]
catho-ap7-3825e [149+1/80, 1]
catho-AP12-3715i [Guardian]
5 m
10 ft

NOTE: The floorplan map type is only available with the NMS-ADV license. For additional information, see Advanced Map Features.

- Geographic — The Geographic map shows a global or regional view where network locations are shown geographically. This map is useful for networks spread across large geographical areas or as a top-level map used to organize multiple networks in different locations.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



This Help topic provides the following information for **Maps**.

- Navigating Maps
  - World Map Navigation Tree
  - Main Map View
  - Viewing Alarm/Device Status
  - Accessing Device Information
  - Link Information
  - Network Details Section
- Performing a Search
  - Finding a Wireless Client
  - Finding an Access Point

  - Finding a Device
  - Finding a Wired Client
- Using Map Links

For information on creating maps, see How to Create and Edit Maps.

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

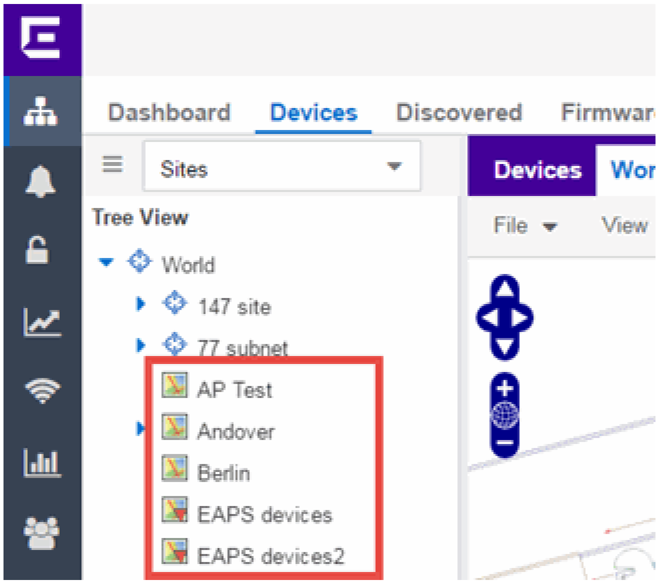
To view or search Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

After you create a map, you can then make it a site. Sites allow you to set a default configuration for devices added to your network.

Navigating the Map Tab

World Map Navigation Tree

As you create your maps, they appear in the **Network** > **Devices** tab navigation tree by selecting **Sites**, nested under the map you configure as the **Parent Map**.



As shown in the image above, you also have the ability to nest maps within other maps. This allows you to organize certain maps as a subset of other maps (for example, creating a building map and then creating a map for each of the floors of the building).

Create Map

Right-click a map in the right-panel navigation tree and select **Maps** > **Create New Map** to create a new map. The first map you create is nested under the World Map. All subsequent maps are nested under the map you right-click when creating the new map.

Edit Map

Right-click a map in the navigation tree and select **Maps** > **Edit Map** to open an existing map in edit mode. Edit mode allows you to add new or move existing devices, APs, and map links on a map.

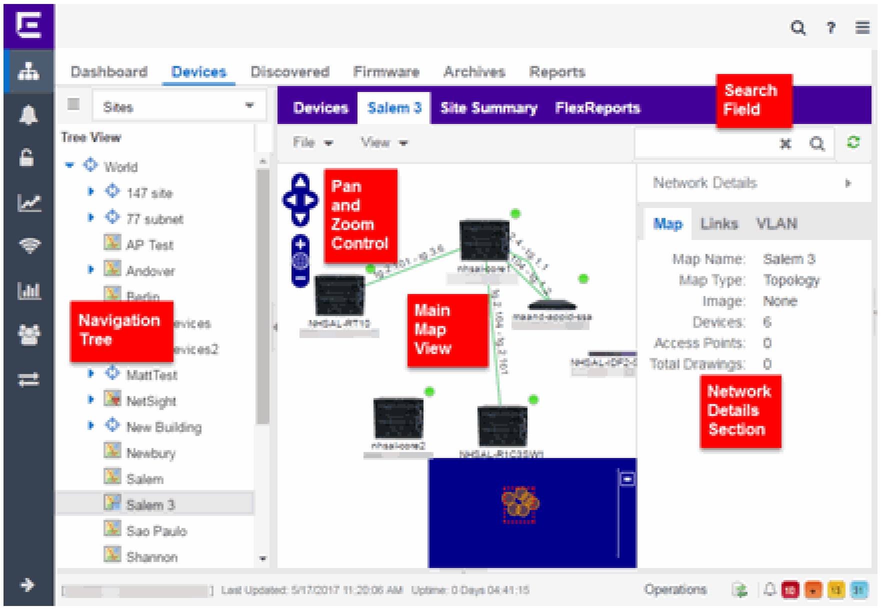
Import Map

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

Main Map View

The Main Map view displays your map with all of the devices, network connections, links, or APs, depending on the type of map. In the Main Map view, you can reorganize the orientation of elements in your map and view the status and details of the elements within the map. The Main Map view also contains the following controls for working with maps:

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



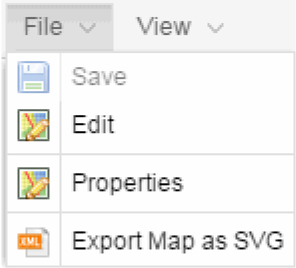
Map Name: Salem 3
Map Type: Topology
Image: None
Devices: 6
Access Points: 0
Total Drawings: 0

Last Updated: 5/17/2017 11:20:06 AM Uptime: 0 Days 04:41:15

File, View, and Tool Menus

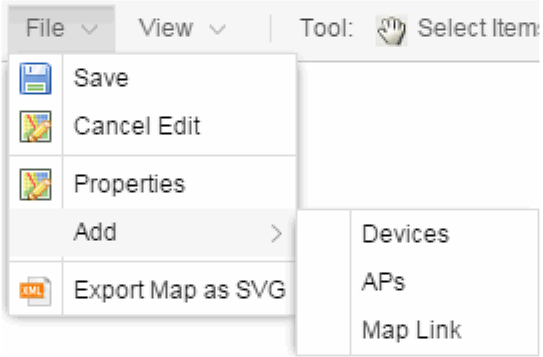
File Menu

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



NOTE: To change the image used for a device type in a map, right-click the device and select Customize Device Type Image. The Upload Custom Device Type Image window appears where you can drag and drop the new image file. The height and width of image files must be less than 1,000 pixels.

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



Clicking **Properties** opens the Map Properties window, which allows you to view and edit information about the map, including the map type, name, and background image. With an NMS-ADV license, the **Export Map as SVG** and **Export Map as ZIP** options are available in the **File** menu, which allow you to export the map in SVG or ZIP format, respectively.

When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated with those devices, your SVG file is identical to the view on your screen; displaying the two devices surrounded by boxes containing the VLAN names. To save the SVG file locally, right-click the map and select **Save as**.

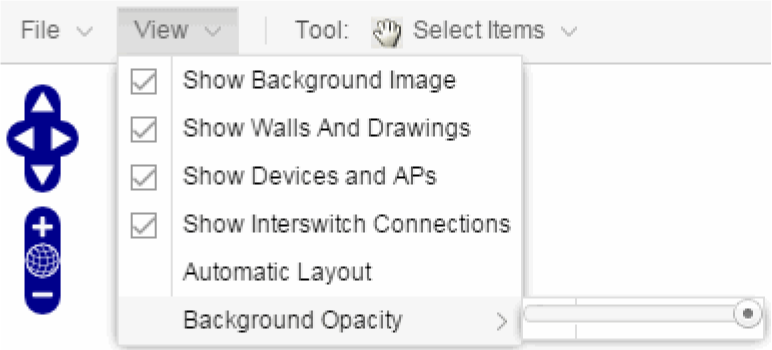
NOTE: For additional information regarding displaying VLANs in a map, see the VLAN tab section.

Only floorplan maps can be exported as a ZIP file. Floorplan maps you export as a ZIP file are typically used to import a floorplan into another instance of Extreme Management Center.

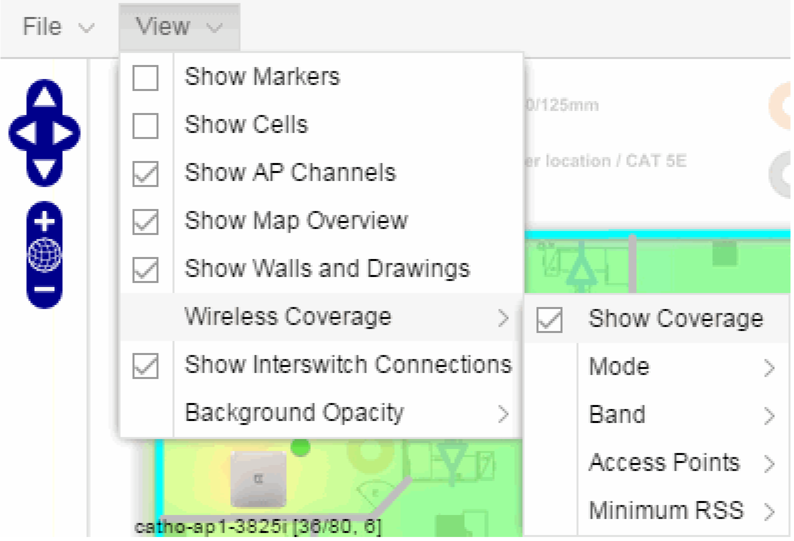
Additionally, by clicking **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Click **Cancel Edit** to exit Edit mode. If you made any changes to the map, a dialog box appears from which you can choose to save the changes or exit Edit mode without saving your changes.

View Menu

The **View** menu allows you to show or hide parts of your map. The options in the **View** menu do not change the information in the map, only allow you to show or hide additional information.



These options vary depending on the map Type. For example, floorplan maps display additional options, including the image you selected as the background of your map, the grid cells that establish the scale of the floorplan, the AP channels for floorplans, the map overview, the walls and drawings of the building, the wireless coverage within a floorplan, the interswitch connections, and the opacity of the background image.



NOTE: The floorplan map type is only available with the NMS-ADV license. For additional information, see Advanced Map Features.

Tool Menu

The **Tool** menu allows you to add lines and shapes to your maps. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
🖐	**Select Items** Click on a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Click anywhere on the map and drag to reposition the map image.
⬠	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.
▭	**Draw Rectangle** Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
✎	**Add Text** Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click to add the text to your map. Use the **Style** menu to change the text appearance.
△	**Draw Triangle** Position the cursor where you want the triangle. Click and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
⟋	**Draw Line** Position your cursor where you want to start drawing the line. Click once and draw the line. Click to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
↻	**Rotate Shape** Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)

Pan and Zoom Control

Pan Control

The **Pan** control allows you to move left/right and up/down in the map. You can also change the position of the map by clicking and dragging the map in any direction.

Zoom Control

The **Zoom** control lets you zoom in and out of the map. You can also zoom in and out of the map by rotating the mouse scroll wheel forward and backward, respectively. Clicking the globe icon in the center of the **Zoom** control resets the zoom and positioning for the map to the last view configured in edit mode.

NOTE: Changing the location and zoom using these controls and then saving the map saves those orientation changes to the map.

Search Field

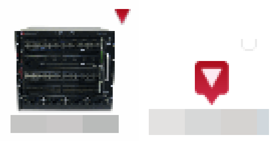
The **Search** field allows you to search for a wireless client, an AP, or for a device or wired client. Enter a MAC address, IP address, hostname, user name, or AP serial number in the **Search** field and press **Enter** to start a search for a device or wired client.

Clicking the **Refresh** button 🔄 to the right of the **Search** field refreshes the map, including the position of mobile devices connected to an AP. When you click the **Refresh** button, the position of mobile devices updates according to their most recent location.

For additional information, see Performing a Search.

Viewing Alarm/Device Status

Maps display an integrated alarm/device status either to the right of a device or AP image, or incorporated as part of a map marker (if you have **Show Markers** selected from the map View menu). For example, the device below is down and a critical alarm is triggered (shown as a device image and as a marker).



Alarm status automatically updates every 30 seconds. Change this status refresh interval in the Extreme Management Center options (Administration > Options > OneView > Map).

- ▼ (Red) Critical — There is a critical alarm and the device is down.
- ▶ (Orange) Error — There is a problem with limited implications on the device.
- ▲ (Yellow) Warning — There is a condition that might lead to a problem on the device.
- ■ (Blue) Info — There is an information-only alarm on the device.
- ● (Green) Clear — There are no alarms and the device is up.

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

Accessing Device Information

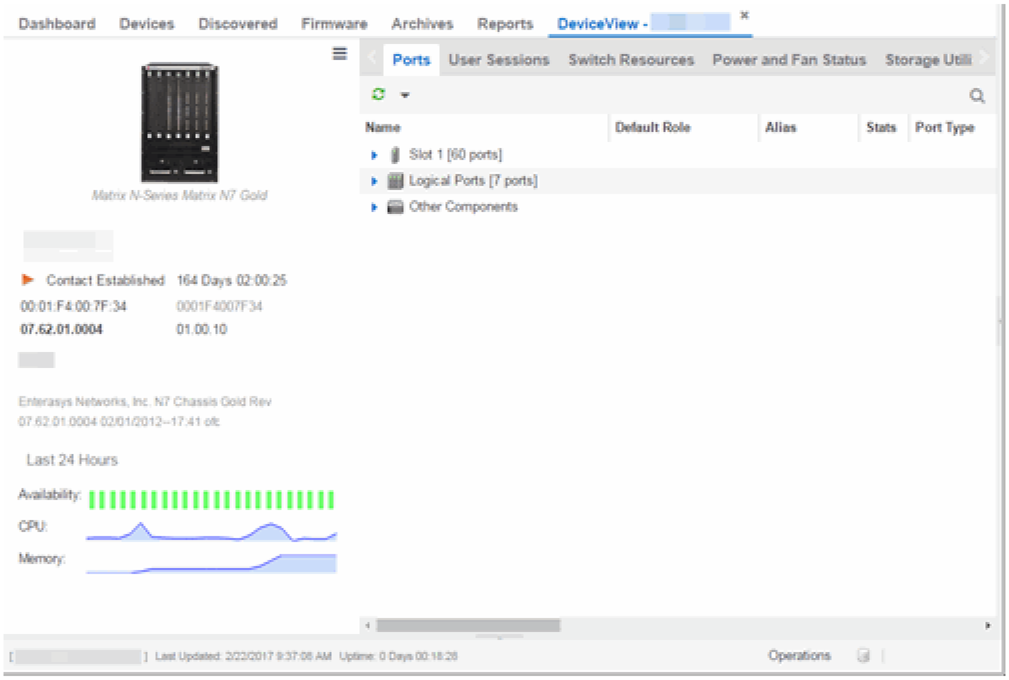
There are two ways to access additional device information from a map.

Device Reports

Launch device information reports from a right-click menu on a device or AP in a map. The menu displays different options based on the device type. You must be in Edit mode to see the **Remove From Map** option.

Device/AP Details

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



Name	Default Role	Alias	Stats	Port Type
Slot 1 [60 ports]				
Logical Ports [7 ports]				
Other Components				

Matrix N-Series Matrix N7 Gold

Contact Established 164 Days 02:00:25
00:01:F4:00:7F:34 0001F4007F34
07.62.01.0004 01.00.10

Enterasys Networks, Inc. N7 Chassis Gold Rev 07.62.01.0004 02/01/2012--17:41 ofc

Last 24 Hours
Availability:
CPU:
Memory:

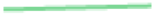
[ ] Last Updated: 2/22/2017 9:37:08 AM Uptime: 0 Days 00:18:28

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

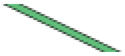
Link Information

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

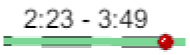
- Basic links appear as thin green lines with no outlining.



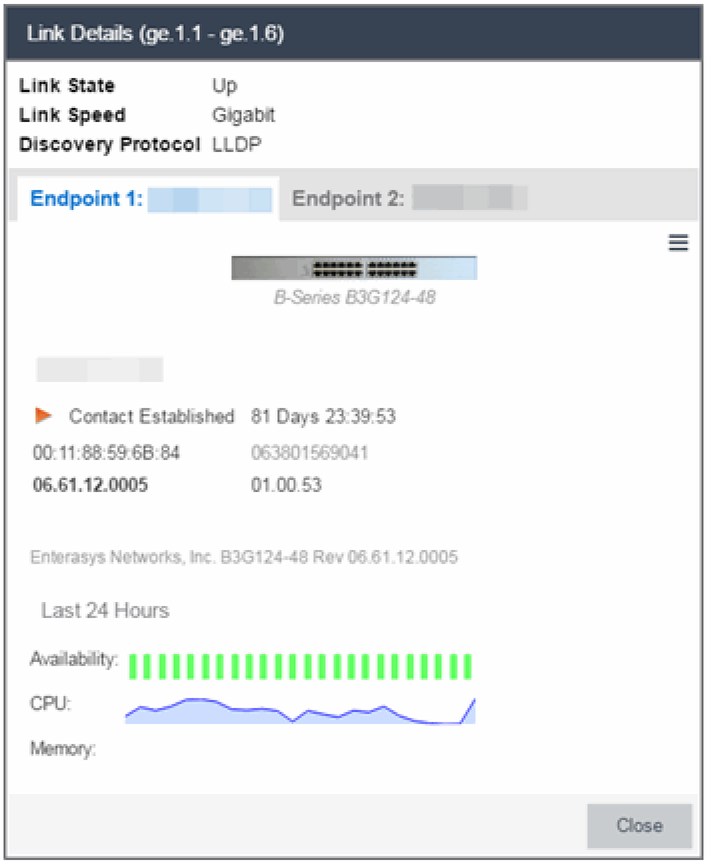
- Shared links appear as basic links when the EAPS domain is not highlighted and appear as thick green lines outlined by a black solid line when you highlight the associated EAPS domain.
- Lag links also appear as thick green lines outlined by a black solid line, but are thicker than shared links and 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.



Link Details (ge.1.1 - ge.1.6)

Link State	Up
Link Speed	Gigabit
Discovery Protocol	LLDP

Endpoint 1: [redacted] **Endpoint 2:** [redacted]

B-Series B3G124-48

[redacted]

Contact Established	81 Days 23:39:53
00:11:88:59:6B:84	063801569041
06.61.12.0005	01.00.53

Enterasys Networks, Inc. B3G124-48 Rev 06.61.12.0005

Last 24 Hours

Availability:

CPU:

Memory:

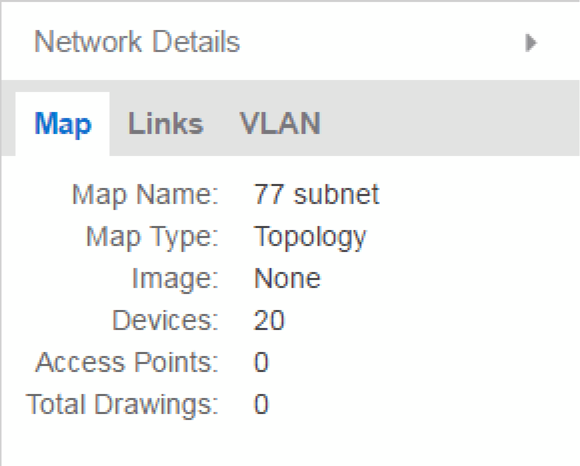
Network Details Section

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

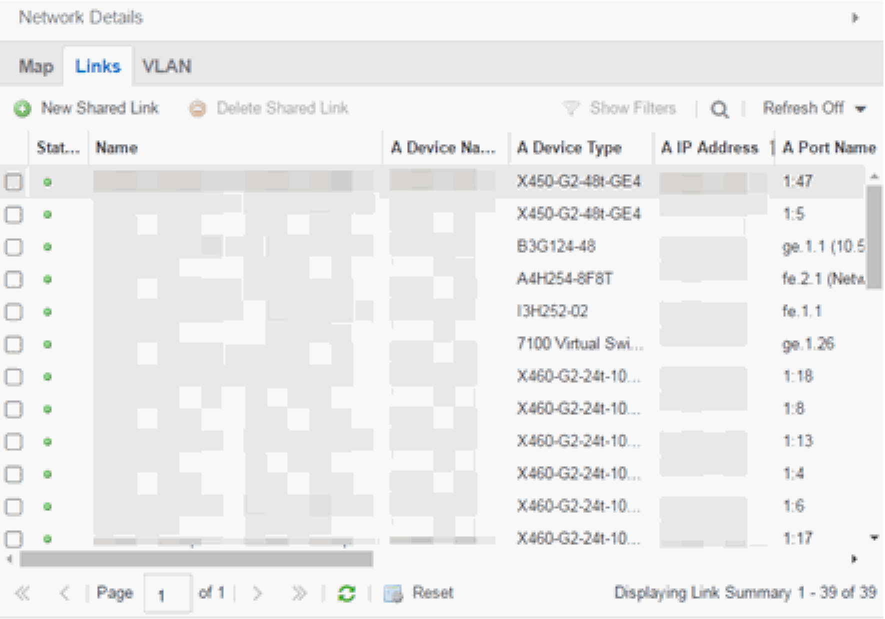
The **Map** tab displays basic information about the map, including the name of the map, the map type, and the background image, as well as the number of devices, APs, and drawings on the map.



Map Name:	77 subnet
Map Type:	Topology
Image:	None
Devices:	20
Access Points:	0
Total Drawings:	0

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.



	Stat...	Name	A Device Na...	A Device Type	A IP Address	A Port Name
□	●	[redacted]	[redacted]	X450-G2-48t-GE4	[redacted]	1:47
□	●	[redacted]	[redacted]	X450-G2-48t-GE4	[redacted]	1:5
□	●	[redacted]	[redacted]	B3G124-48	[redacted]	ge.1.1 (10.5
□	●	[redacted]	[redacted]	A4H254-8F8T	[redacted]	fe.2.1 (Netw
□	●	[redacted]	[redacted]	I3H252-02	[redacted]	fe.1.1
□	●	[redacted]	[redacted]	7100 Virtual Swi...	[redacted]	ge.1.26
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:18
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:8
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:13
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:4
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:6
□	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:17

Displaying Link Summary 1 - 39 of 39

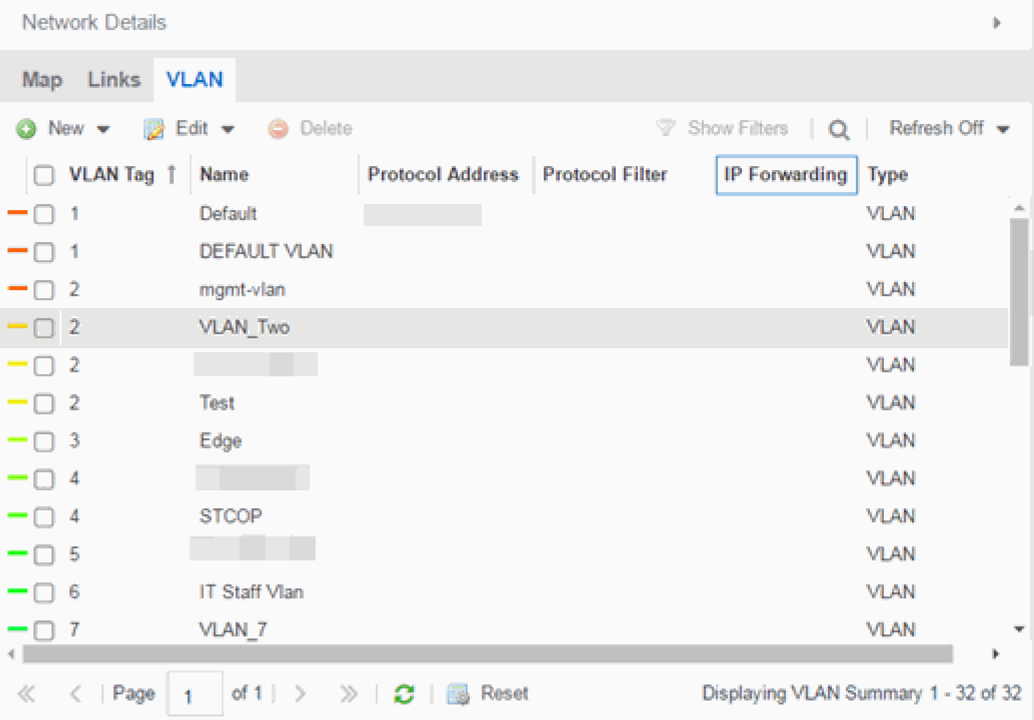
The top of the **Links** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

Double-clicking a link opens the Link Details window.

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

VLAN tab

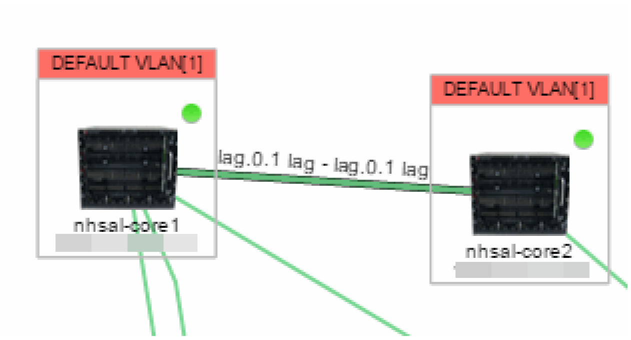
The **VLAN** tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled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



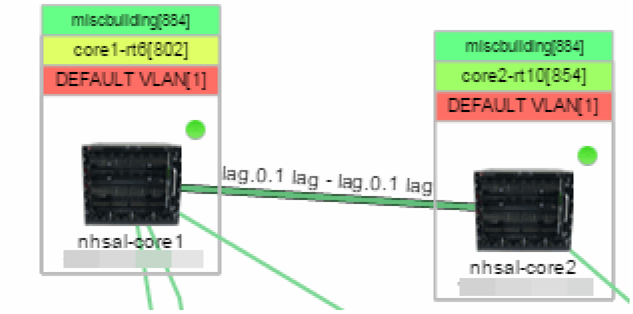
	□	VLAN Tag ↑	Name	Protocol Address	Protocol Filter	IP Forwarding	Type
🟧	□	1	Default	[redacted]			VLAN
🟧	□	1	DEFAULT VLAN				VLAN
🟧	□	2	mgmt-vlan				VLAN
🟨	□	2	VLAN_Two				VLAN
🟨	□	2	[redacted]				VLAN
🟨	□	2	Test				VLAN
🟩	□	3	Edge				VLAN
🟩	□	4	[redacted]				VLAN
🟩	□	4	STCOP				VLAN
🟩	□	5	[redacted]				VLAN
🟩	□	6	IT Staff Vlan				VLAN
🟩	□	7	VLAN_7				VLAN

Displaying VLAN Summary 1 - 32 of 32

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.



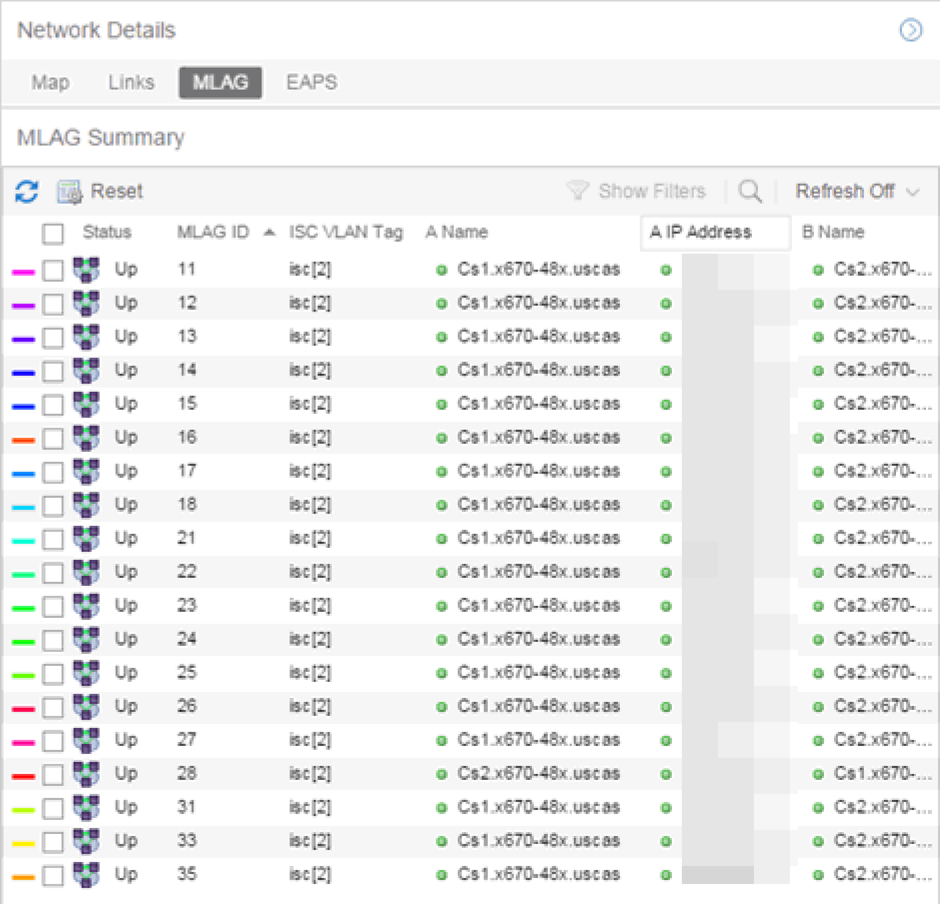
Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.



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

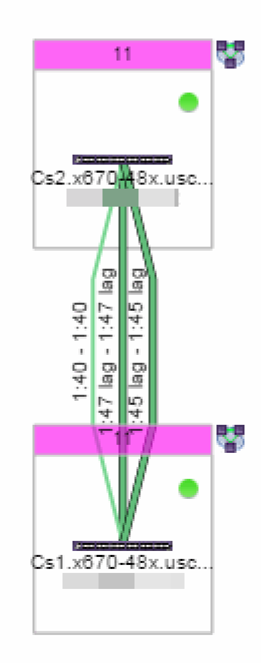
The **MLAG** tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of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



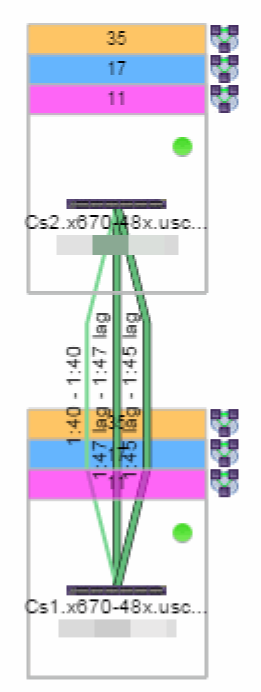
MLAG Summary

	☐	Status	MLAG ID ▲	ISC VLAN Tag	A Name	A IP Address	B Name
▬	☐	Up	11	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	12	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	13	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	14	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	15	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	16	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	17	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	18	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	21	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	22	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	23	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	24	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	25	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	26	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	27	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	28	isc[2]	● Cs2.x670-48x.uscas	● [redacted]	● Cs1.x670-...
▬	☐	Up	31	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	33	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
▬	☐	Up	35	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...

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.

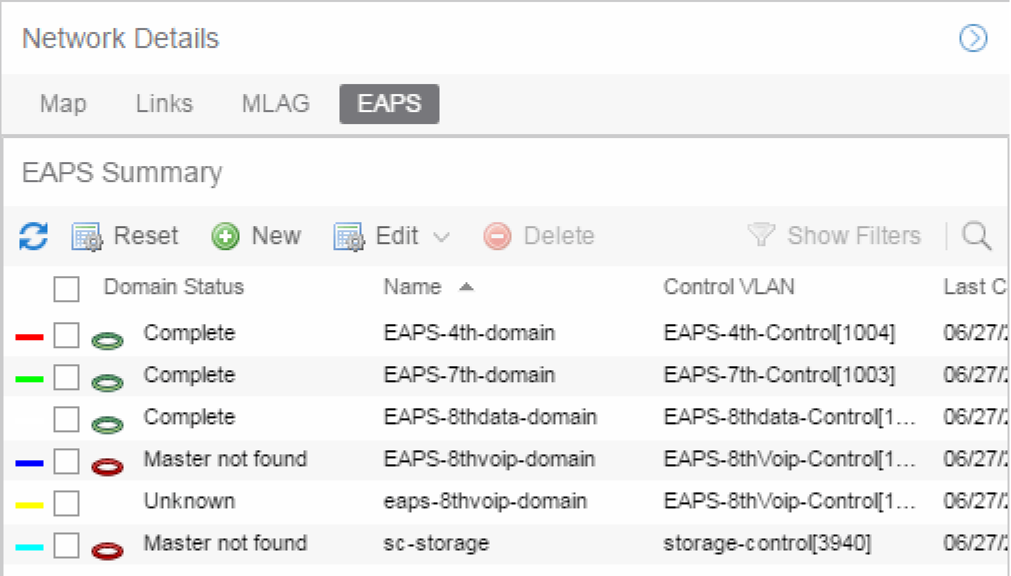


Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.



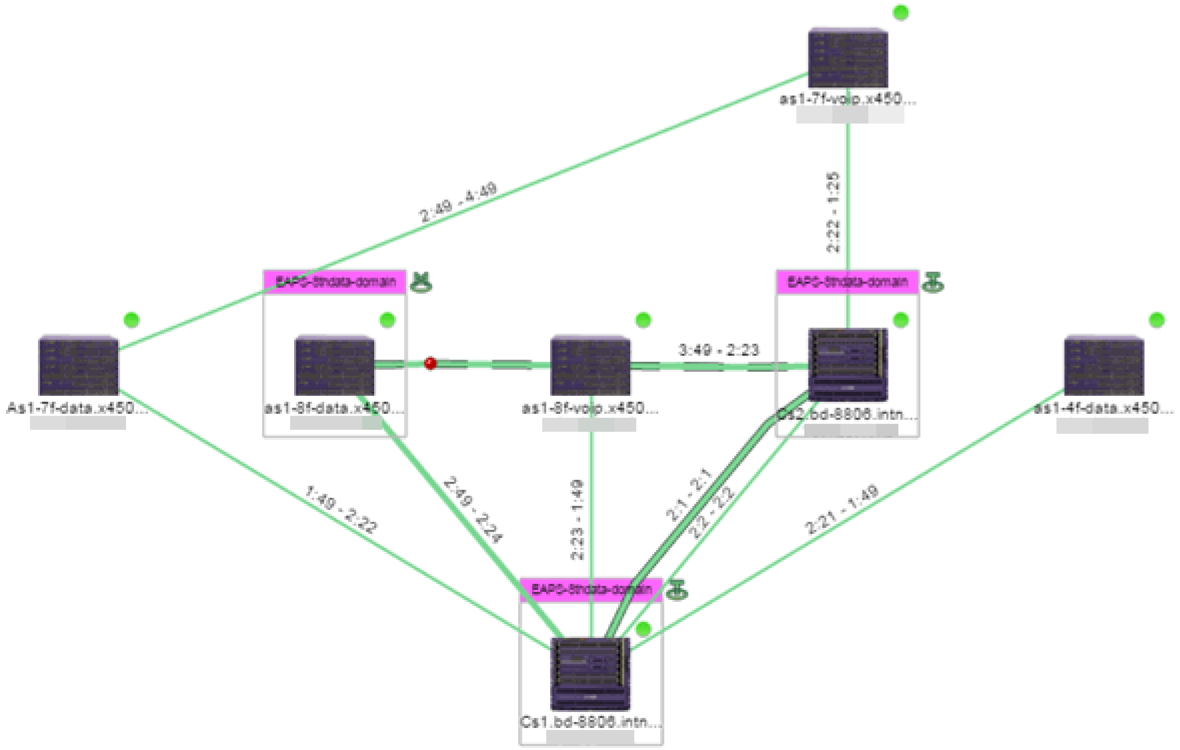
EAPS tab

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.

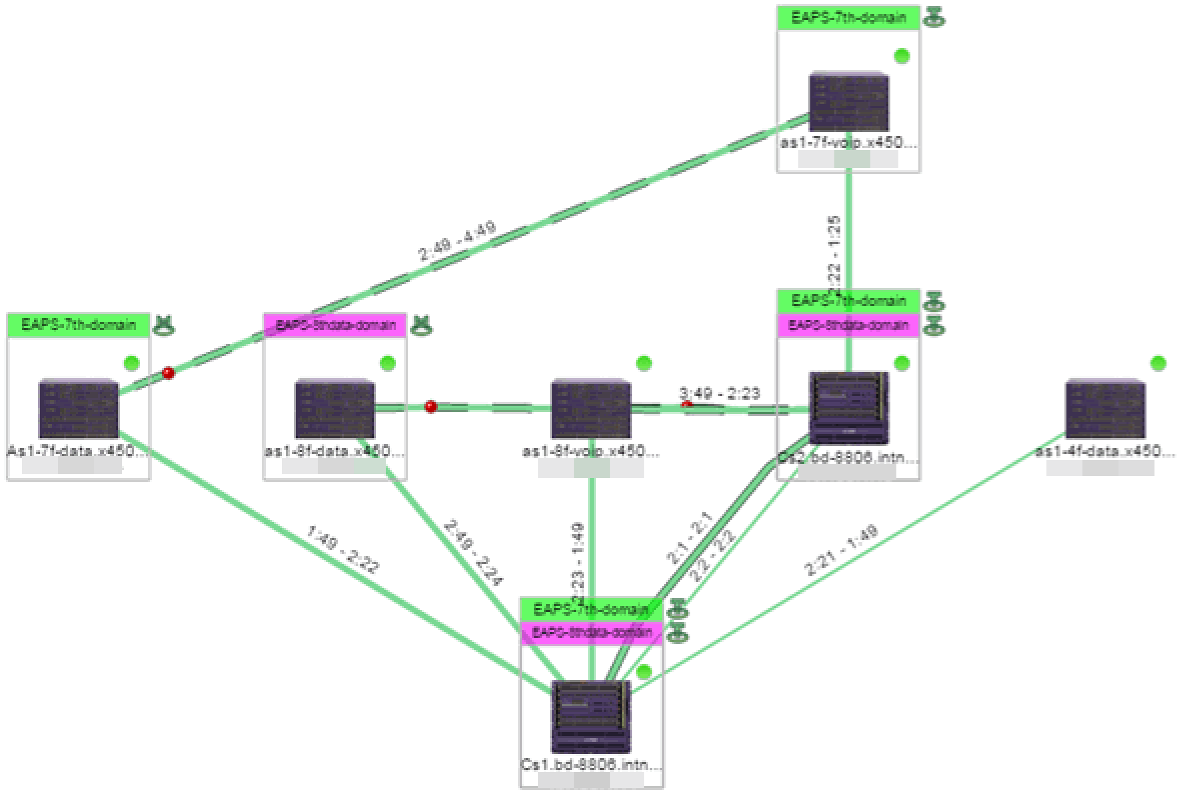


	□	Domain Status	Name ▲	Control VLAN	Last C
🟥	□	Complete	EAPS-4th-domain	EAPS-4th-Control[1004]	06/27/
🟩	□	Complete	EAPS-7th-domain	EAPS-7th-Control[1003]	06/27/
	□	Complete	EAPS-8thdata-domain	EAPS-8thdata-Control[1...	06/27/
🟦	□	Master not found	EAPS-8thvoip-domain	EAPS-8thVoip-Control[1...	06/27/
🟨	□	Unknown	eaps-8thvoip-domain	EAPS-8thVoip-Control[1...	06/27/
🟦	□	Master not found	sc-storage	storage-control[3940]	06/27/

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.

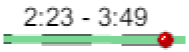


An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

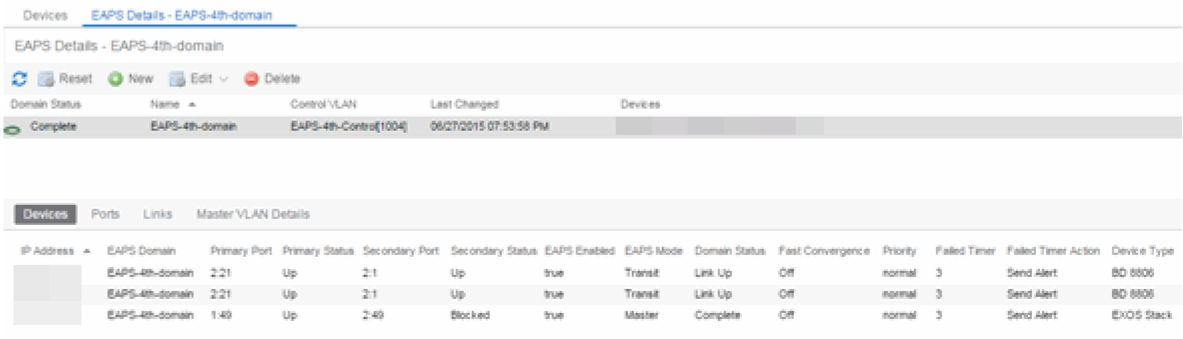
The color of the ring icon indicates the status of the domain:

- 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.



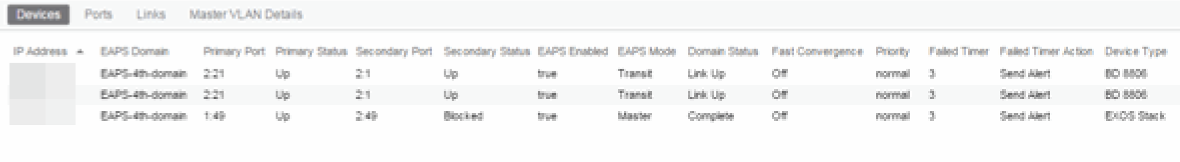
EAPS Details - EAPS-4th-domain

Domain Status	Name	Control VLAN	Last Changed	Devices
Complete	EAPS-4th-domain	EAPS-4th-Control[1004]	06/27/2015 07:53:58 PM	[redacted]

IP Address	EAPS Domain	Primary Port	Primary Status	Secondary Port	Secondary Status	EAPS Enabled	EAPS Mode	Domain Status	Fast Convergence	Priority	Failed Timer	Failed Timer Action	Device Type
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	1:49	Up	2:49	Blocked	true	Master	Complete	Off	normal	3	Send Alert	EXOS Stack

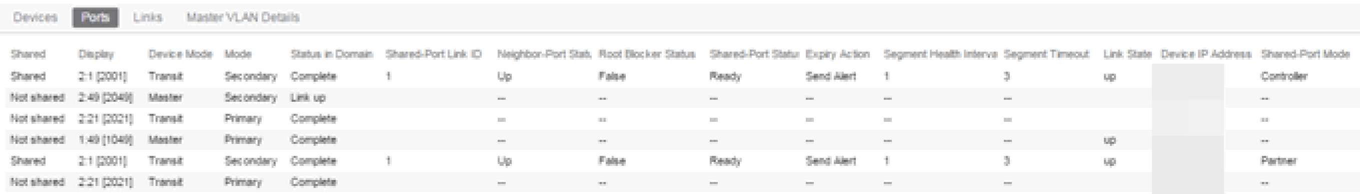
The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

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



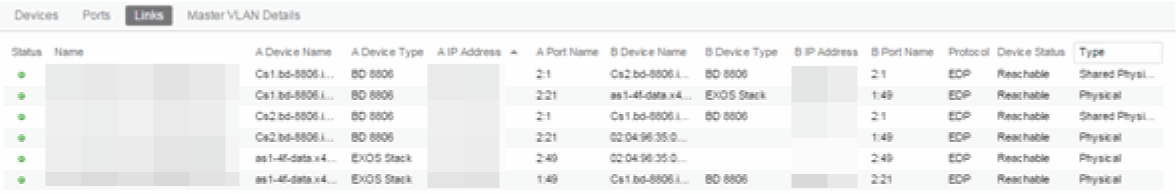
IP Address	EAPS Domain	Primary Port	Primary Status	Secondary Port	Secondary Status	EAPS Enabled	EAPS Mode	Domain Status	Fast Convergence	Priority	Failed Timer	Failed Timer Action	Device Type
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	1:49	Up	2:49	Blocked	true	Master	Complete	Off	normal	3	Send Alert	EXOS Stack

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



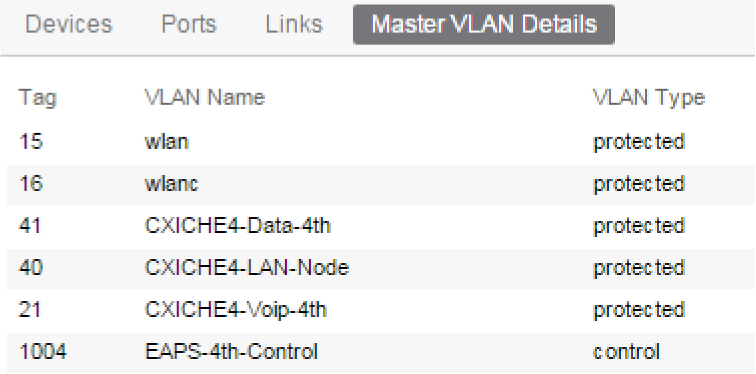
Shared	Display	Device Mode	Mode	Status in Domain	Shared-Port Link ID	Neighbor-Port Stat.	Root Blocker Status	Shared-Port Statu	Expiry Action	Segment Health Interva	Segment Timeout	Link State	Device IP Address	Shared-Port Mode
Shared	2:1 [2001]	Transit	Secondary	Complete	1	Up	False	Ready	Send Alert	1	3	up	[redacted]	Controller
Not shared	2:49 [2049]	Master	Secondary	Link up		--	--	--	--	--	--		[redacted]	--
Not shared	2:21 [2021]	Transit	Primary	Complete		--	--	--	--	--	--		[redacted]	--
Not shared	1:49 [1049]	Master	Primary	Complete		--	--	--	--	--	--	up	[redacted]	--
Shared	2:1 [2001]	Transit	Secondary	Complete	1	Up	False	Ready	Send Alert	1	3	up	[redacted]	Partner
Not shared	2:21 [2021]	Transit	Primary	Complete		--	--	--	--	--	--		[redacted]	--

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



Status	Name	A Device Name	A Device Type	A IP Address	A Port Name	B Device Name	B Device Type	B IP Address	B Port Name	Protocol	Device Status	Type
●	[redacted]	Cs1.bd-8806.i...	BD 8806	[redacted]	2:1	Cs2.bd-8806.i...	BD 8806	[redacted]	2:1	EDP	Reachable	Shared Physi...
●	[redacted]	Cs1.bd-8806.i...	BD 8806	[redacted]	2:21	as1-4f-data.x4...	EXOS Stack	[redacted]	1:49	EDP	Reachable	Physical
●	[redacted]	Cs2.bd-8806.i...	BD 8806	[redacted]	2:1	Cs1.bd-8806.i...	BD 8806	[redacted]	2:1	EDP	Reachable	Shared Physi...
●	[redacted]	Cs2.bd-8806.i...	BD 8806	[redacted]	2:21	02:04:96:35:0...		[redacted]	1:49	EDP	Reachable	Physical
●	[redacted]	as1-4f-data.x4...	EXOS Stack	[redacted]	2:49	02:04:96:35:0...			2:49	EDP	Reachable	Physical
●	[redacted]	as1-4f-data.x4...	EXOS Stack	[redacted]	1:49	Cs1.bd-8806.i...	BD 8806	[redacted]	2:21	EDP	Reachable	Physical

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



Tag	VLAN Name	VLAN Type
15	wlan	protected
16	wlanc	protected
41	CXICHE4-Data-4th	protected
40	CXICHE4-LAN-Node	protected
21	CXICHE4-Voip-4th	protected
1004	EAPS-4th-Control	control

Clicking the **New EAPS Domain** button opens the New EAPS Domain wizard, which allows you to create a new EAPS domain. For additional information, see How to Create a New EAPS Domain.

Performing a Search

You can search for a wireless client, an AP, a device, or a wired client on the **Search** tab. From the tab, select **Search Maps** from the Search drop-down menu, enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information, and press **Enter**.

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

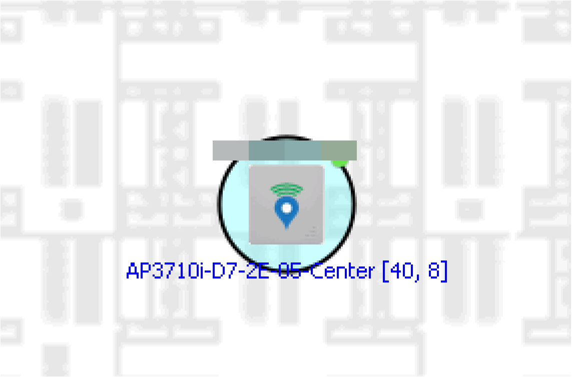
Finding a Wireless Client

From the Search Field on the Network Tab

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

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

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



From the Wireless Tab

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

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

Radius Distance Calculation

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

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

where:

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

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

where:

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

Finding an Access Point

From the Wireless Tab

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

From the Reports Page

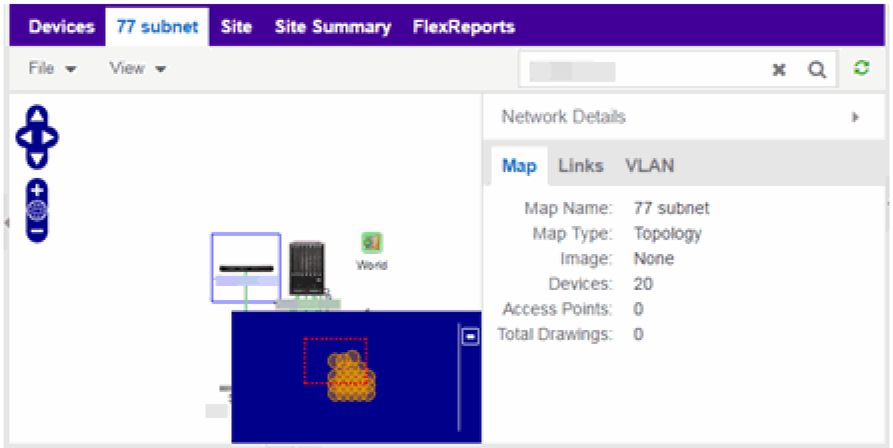
You can locate an AP from the Wireless > APs Summary report on the **Reports** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

Finding a Device

From the Network Page Search Field

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

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



Map Name: 77 subnet
Map Type: Topology
Image: None
Devices: 20
Access Points: 0
Total Drawings: 0

Finding a Wired Client

From the Network Tab Search Field

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

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

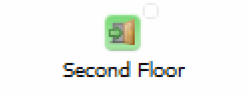
From the Control Tab

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

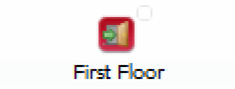
Using Map Links

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

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



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



Additionally, you can use map links to display Application data based on Application Analytics network locations. For additional information, see Advanced Map Features.

Related Information

For information on related topics:

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

How to Create and Edit Maps

The Extreme Management Center Maps feature lets you create maps of the devices and wireless access points (APs) on your network. Begin by selecting a background image to serve as a map, such as a building or floor plan, and then position your managed devices and wireless APs on the map. For example, a typical map might present an office floor plan that shows the location of wireless access points.

For introductory information on maps in Extreme Management Center, see Extreme Management Center Maps.

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

- 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
- Creating a Manual Link Between Devices
- Adding Map Links
- Setting the Map Scale

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

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

Creating a Map

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

1. Launch Extreme Management Center and click on the **Network** tab.
2. Open the **Devices** tab.
3. In the left-panel select **Sites**.

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

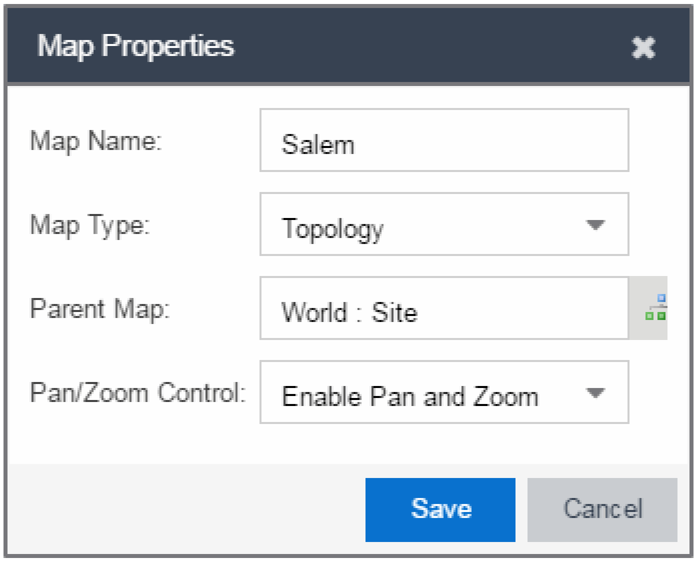
> **NOTE:** You cannot create a new map if you are currently editing another map.

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

   A new map is added to the tree underneath the map you selected and the Maps section of the window opens.

   The new map is initially blank unless you create it from a device or AP by selecting the device or AP, clicking the **Menu** icon (☰) or right-clicking the device or AP and selecting **Maps** > **Create Map**. To begin adding devices, APs and links to the map, proceed to Step 7. Proceed to the following step to edit the map properties.

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



Map Properties

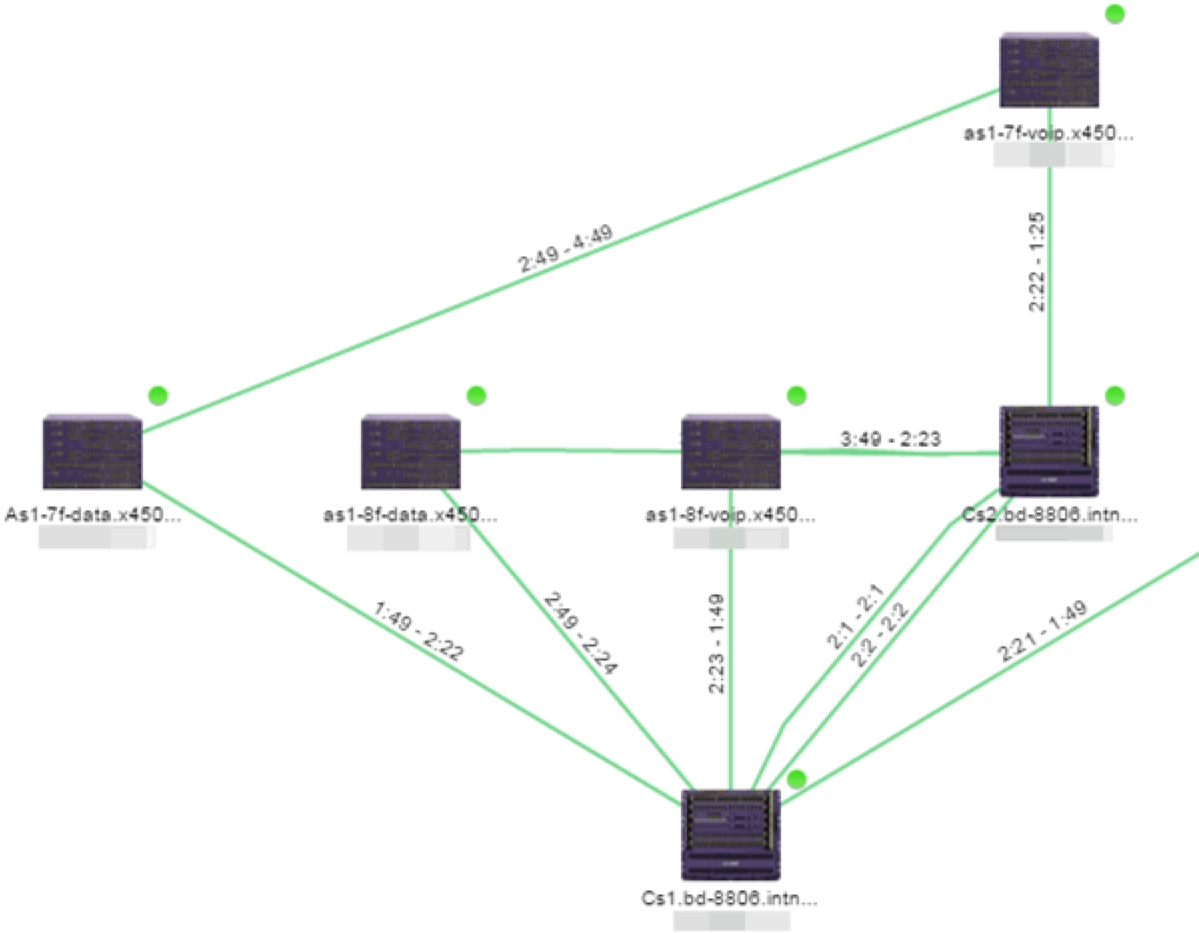
Map Name: Salem

Map Type: Topology

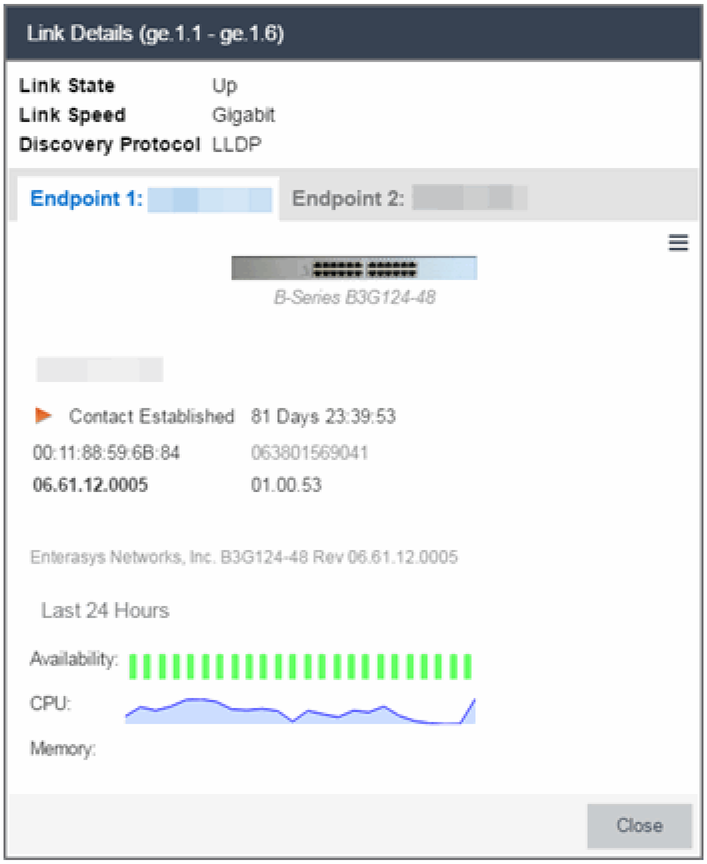
Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

   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.



Link Details (ge.1.1 - ge.1.6)

Link State Up
Link Speed Gigabit
Discovery Protocol LLDP

[redacted]

Contact Established 81 Days 23:39:53
00:11:88:59:6B:84 063801569041
06.61.12.0005 01.00.53

Enterasys Networks, Inc. B3G124-48 Rev 06.61.12.0005

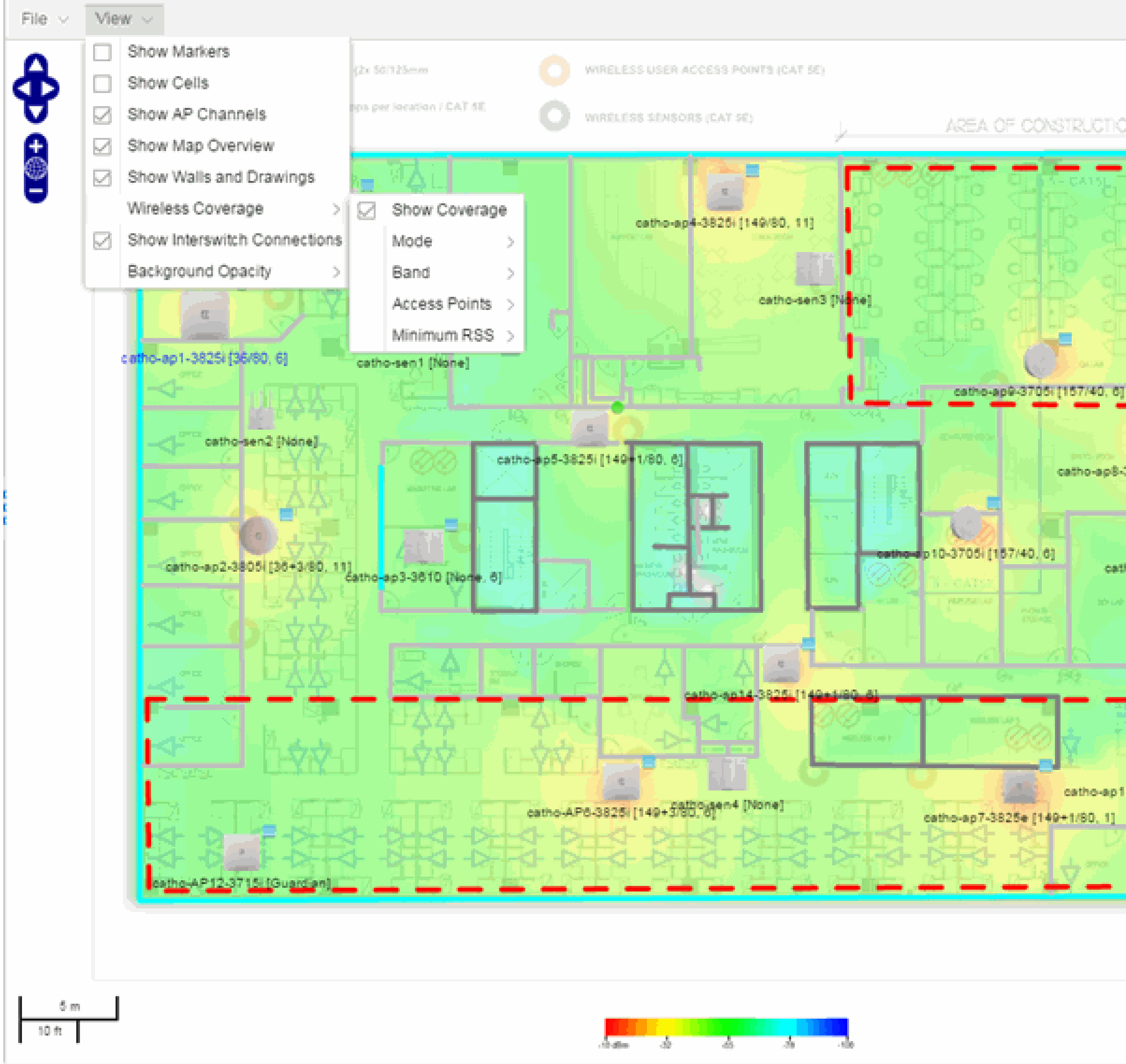
- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in the .png, .gif, and .jpg format. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed. To use an image larger than 3,000 x 2,000 pixels, open the `NSJBoss.properties` file and edit the pixel value of the `oneView.maxImageSize=3000x2000` line.

CAUTION: Increasing the oneView.maxImageSize value may cause stability issues.

If you select this option, a **Map Image** field displays under the **Map Type** field. In the **Map Image** field, use the drop-down menu to select an image or click the ⊕ button to open a window where you can select a local image and upload it to the Extreme Management Center server.

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

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage >
☑ Show Interswitch Connections
Background Opacity >
☑ Show Coverage
Mode >
Band >
Access Points >
Minimum RSS >
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTIO
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap7-3825e [149+1/80, 1]
catho-AP12-3715i [Guardian]
5 m
10 ft

If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located. If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located.

For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the AP's radio frequencies are not be obstructed by any walls, and the area where a client might be located is larger. See Finding a Wireless Client for more information.

- Open space — The wireless APs are located in an environment with no walls or cubicles.
- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — For customers with a NMS-ADV license, use this option to create custom floor plans. For more information, see Advanced Map Features.

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

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

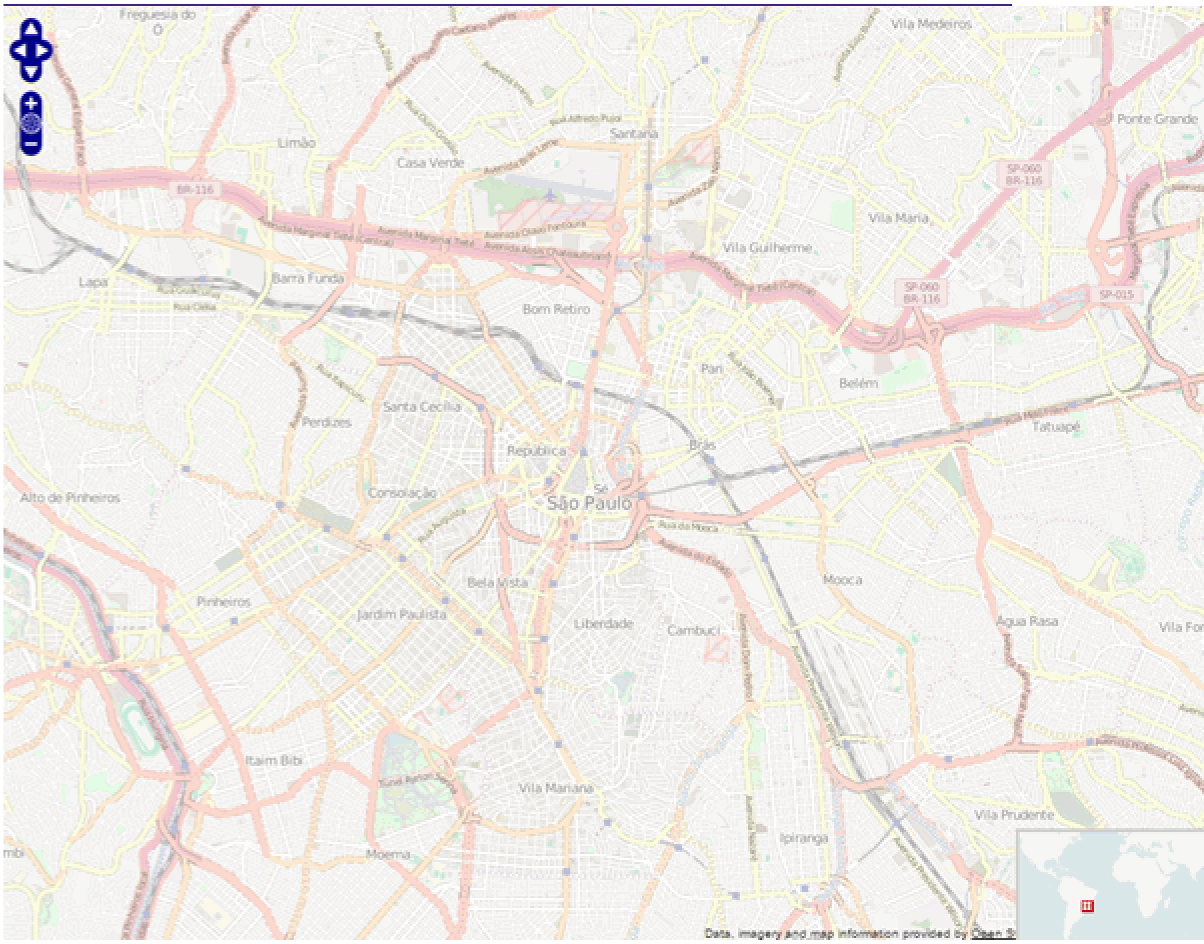
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

The Map feature supports images in the .png, .gif, and .jpg format. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed. To use an image larger than 3,000 x 2,000 pixels, open the `NSJBoss.properties` file and edit the pixel value of the `oneView.maxImageSize=3000x2000` line.

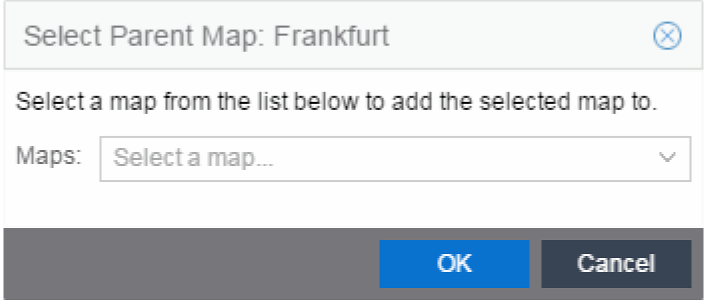
CAUTION: Increasing the oneView.maxImageSize value may cause stability issues and performance issues when generating a heatmap.

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

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



Select Parent Map: Frankfurt

Select a map from the list below to add the selected map to.

Maps: Select a map...

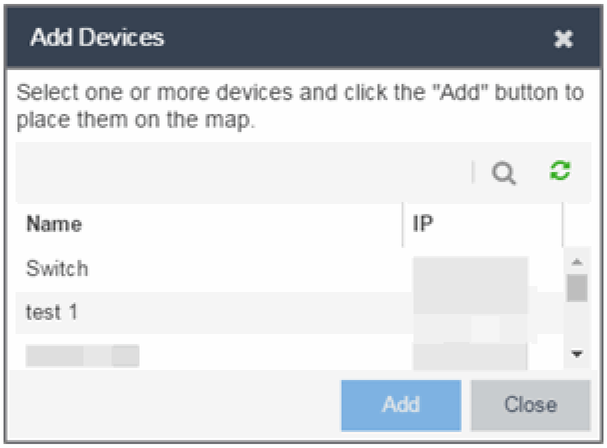
d. Click **Save**.

e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like world or city maps. For example, if a person viewing a map changes the location and zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.

The Pan control allows you to move left/right and up/down in the map.

The Zoom control lets you zoom in and out of the map.

7. Add your devices, APs, or Links to the map you are currently editing by clicking **File** > **Add** > **Devices/APs/Map Link**. This opens the Add window.



Add Devices

Select one or more devices and click the "Add" button to place them on the map.

Name	IP
Switch	[redacted]
test 1	[redacted]
[redacted]	[redacted]

Use the **Search** icon to locate a specific device or AP in the Add Device or Add AP windows, respectively, or select another Map to which to link from the drop-down menu in the Add Link To Map window. Click the **Add** button to add the device, AP, or link to your network map.

8. Once your devices and/or APs are located on your map, manually manipulate the devices, APs, and links on the map, or organize them automatically by clicking **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
   - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.
   - Hierarchical — Organizes devices, APs, and links in a tree pattern.
   - Circular — Organizes devices, APs, and links in a circular pattern.
9. Click **File** > **Save** button to save the map.

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

10. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or click the **Edit** button in the Map Properties panel.

Importing a Map

You can also import a saved map by performing the following steps.

1. Launch Extreme Management Center and click on the **Network** tab.
2. Open the **Devices** tab.
3. Right-click a map in the left-panel Groups/Maps Navigation Tree and select **Maps** > **Import Map**.
   The Import Map window opens.
4. Navigate to the Map file on your local drive or network drive.
5. Configure your import options.
6. Click **Import**.

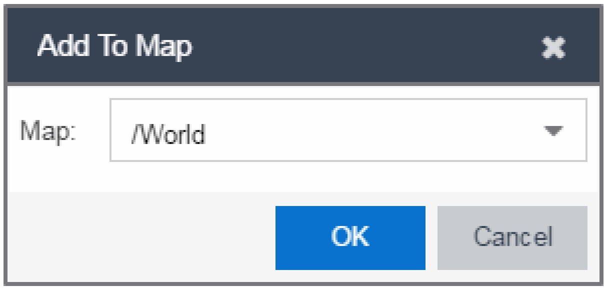
Adding Devices/APs from Extreme Management Center Devices and Wireless

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

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the **Network** tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down menu in the left-panel.
2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Add to Map**.
3. In the Add to Map window, use the drop-down menu to select the desired map. Click **OK** to add the devices or APs to the map.



Map: /World

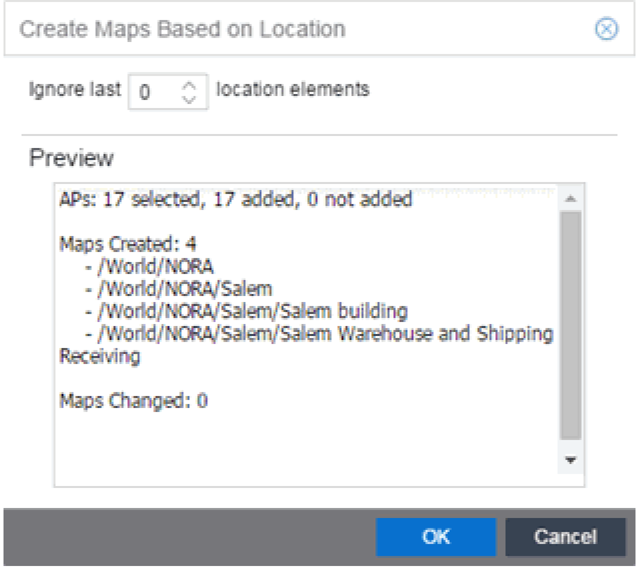
4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be created to the Third Floor level, and then you manually position the devices in the correct location on the map.

1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 9 APs to a map. This creates eight new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.

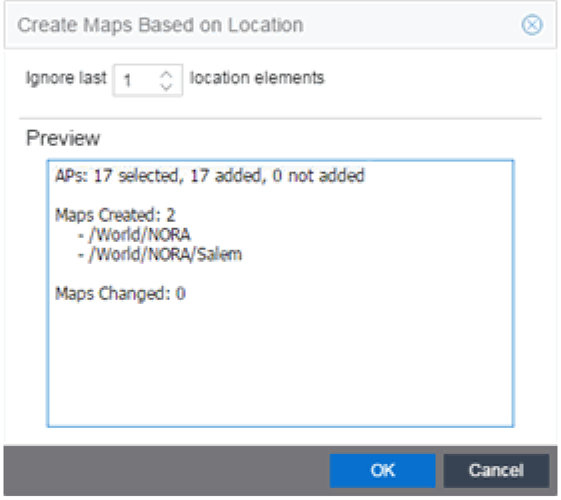
   
   Create Maps Based on Location
Ignore last 0 location elements
Preview
OK
Cancel

   APs: 17 selected, 17 added, 0 not added

   Maps Created: 4
   - /World/NORA
   - /World/NORA/Salem
   - /World/NORA/Salem/Salem building
   - /World/NORA/Salem/Salem Warehouse and Shipping Receiving

   Maps Changed: 0

   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.



APs: 17 selected, 17 added, 0 not added

Maps Created: 2
- /World/NORA
- /World/NORA/Salem

Maps Changed: 0

3. Click **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
5. Click the **Save** button to save the devices/APs to the map.

Creating a Manual Link Between Devices

You can manually create links between devices on a map.

1. Right-click one of the devices to which you are adding the link.
2. Select **Create Link**.

   The Create a Manual Link window displays.
3. Expand the device in the **Name** column of the From Port section of the window and select the port to which the link connects.
4. Select the other device to which the link connects in the **Select Device** drop-down menu.
5. Expand the device in the **Name** column of the To Port section of the window and select the port to which the link connects.
6. Click **OK** to add the link to the map.

NOTES: The **Link State** for a manual link is derived from the **Status** of the ports to which it connects.

Delete a manual link via the Link Details window by double-clicking the link in the map.

Adding Map Links

You can use map links to jump from one map to another. Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating there are no devices with alarms on the Second Floor map.

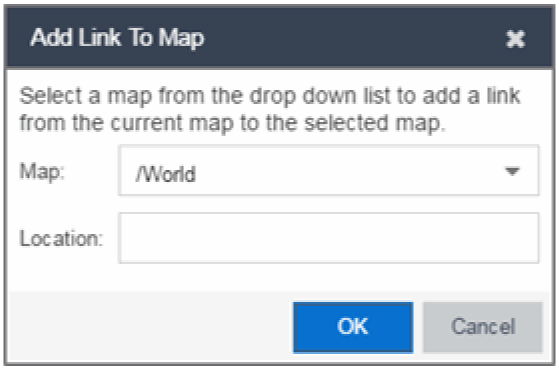
Second Floor

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.

First Floor

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.



Add Link To Map

Select a map from the drop down list to add a link from the current map to the selected map.

Map: /World

Location:

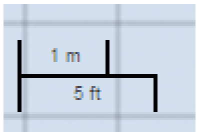
4. From the **Map** drop-down menu, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and click **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Click the **Save** button to save the map and close the properties panel.

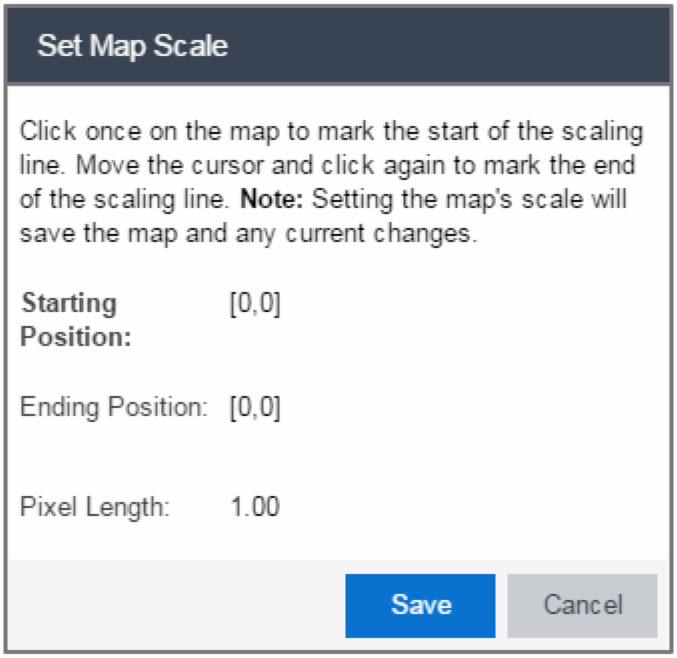
Setting the Map Scale

The map scale appears in the lower left corner of a map and can be changed to accurately reflect your map image.

Use the following steps to set the scale for a map.

1. In the Maps page's navigation tree, right-click on the map and select **Maps** > **Edit Map** or click the **File** > **Edit** button in the map properties panel.
2. Click on the map scale in the map's footer panel to open the Set Map Scale window. (Users with the Extreme Management Center NMS-ADV license can access the Set Map Scale window from the Tools menu.)





Set Map Scale

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. **Note:** Setting the map's scale will save the map and any current changes.

Starting Position: [0,0]

Ending Position: [0,0]

Pixel Length: 1.00

3. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floor plan measure a scaling line on the opening of an office. If you know the office doors are 33 inches wide, enter that as the scaling line measurement.
   a. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
   b. Enter the line length and units.
4. Click Save. The map scale is automatically adjusted and the map is saved.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from Extreme Management Center Devices and Wireless

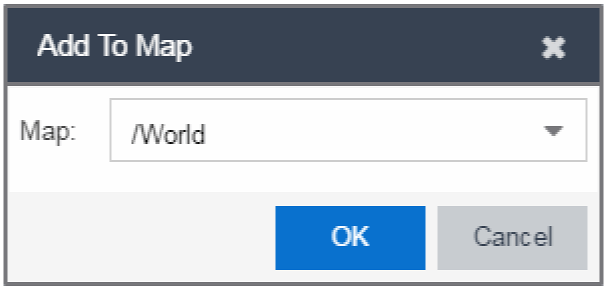
Using the Extreme Management Center Maps feature, you can quickly add devices and wireless access points (APs) to your maps directly from the Devices list or from the navigation tree on the Extreme Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the **Network** tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down menu in the left-panel.
2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Add to Map**.
3. In the Add to Map window, use the drop-down menu to select the desired map. Click **OK** to add the devices or APs to the map.



Map: /World

4. Open the Maps page and select the map to which you added the devices. Right-click

on the map and select **Edit Map**. You can now position the devices as desired.

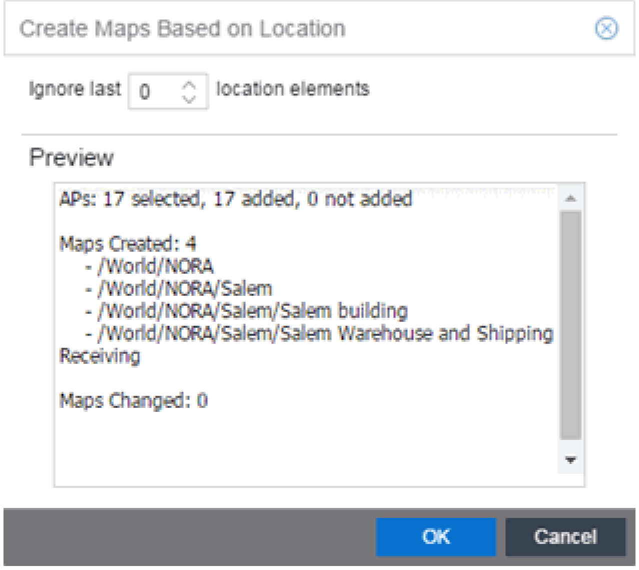
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be created to the Third Floor level, and then you manually position the devices in the correct location on the map.

1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 9 APs to a map. This creates eight new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.



Create Maps Based on Location

Ignore last 0 location elements

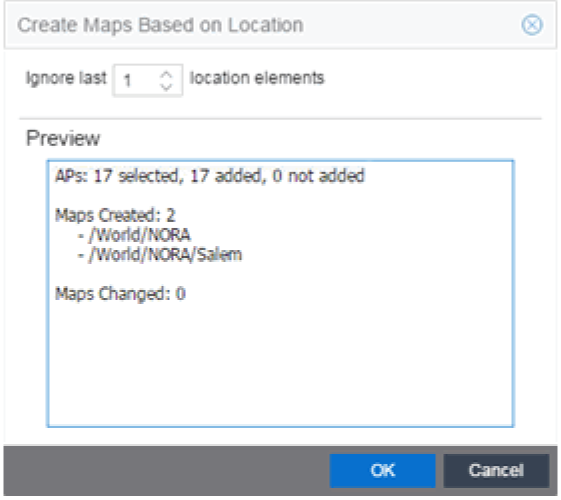
Preview

APs: 17 selected, 17 added, 0 not added

Maps Created: 4
- /World/NORA
- /World/NORA/Salem
- /World/NORA/Salem/Salem building
- /World/NORA/Salem/Salem Warehouse and Shipping Receiving

Maps Changed: 0

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.



APs: 17 selected, 17 added, 0 not added

Maps Created: 2
- /World/NORA
- /World/NORA/Salem

Maps Changed: 0

3. Click **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps.
5. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
6. Click the **Save** button to save the devices/APs to the map.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Create Maps Using the

The Extreme Management Center Maps feature lets you create maps of the devices and wireless access points (APs) on your network. Begin by selecting a background image to serve as a map, such as a building or floor plan, and then position your managed devices and wireless APs on the map. For example, a typical map might present an office floor plan that shows the location of wireless access points.

In order to create maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

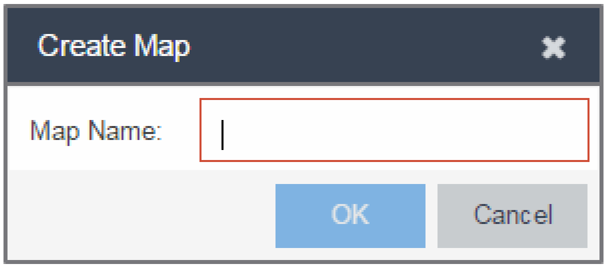
Creating a Map

To create a new Device map:

1. In the left-panel Groups/Maps navigation tree, right-click on the World Site (or any other map in the tree) and select **Maps** > **Create Map**.

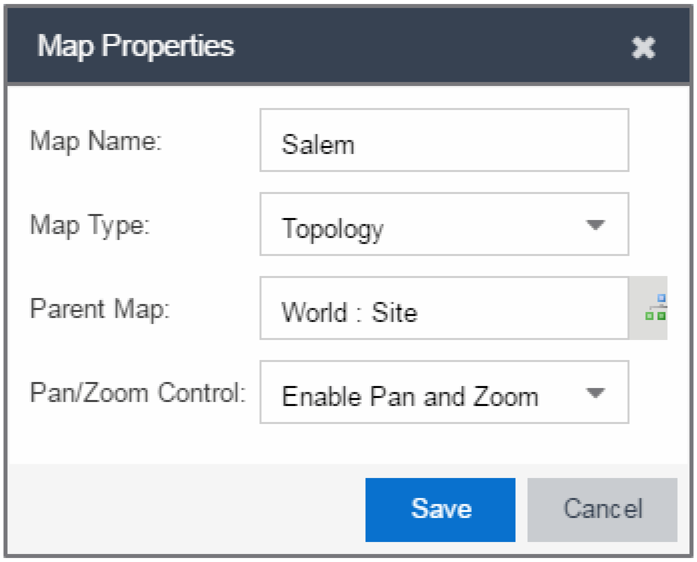
   NOTE: You cannot create a new map if you are currently editing another map.

   The Create Map window, shown below, opens.
2. Enter a name for the map and click **OK**.

   A new map is added to the tree underneath the map you selected and the Maps section of the window opens.

   The new map is initially blank unless you create it from a device or AP by selecting the device or AP, clicking the **Menu** icon (☰) or right-clicking the device or AP and selecting **Maps** > **Create Map**. To begin adding devices, APs and links to the map, proceed to Step 4.
3. Click **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



Map Properties

Map Name: Salem

Map Type: Topology

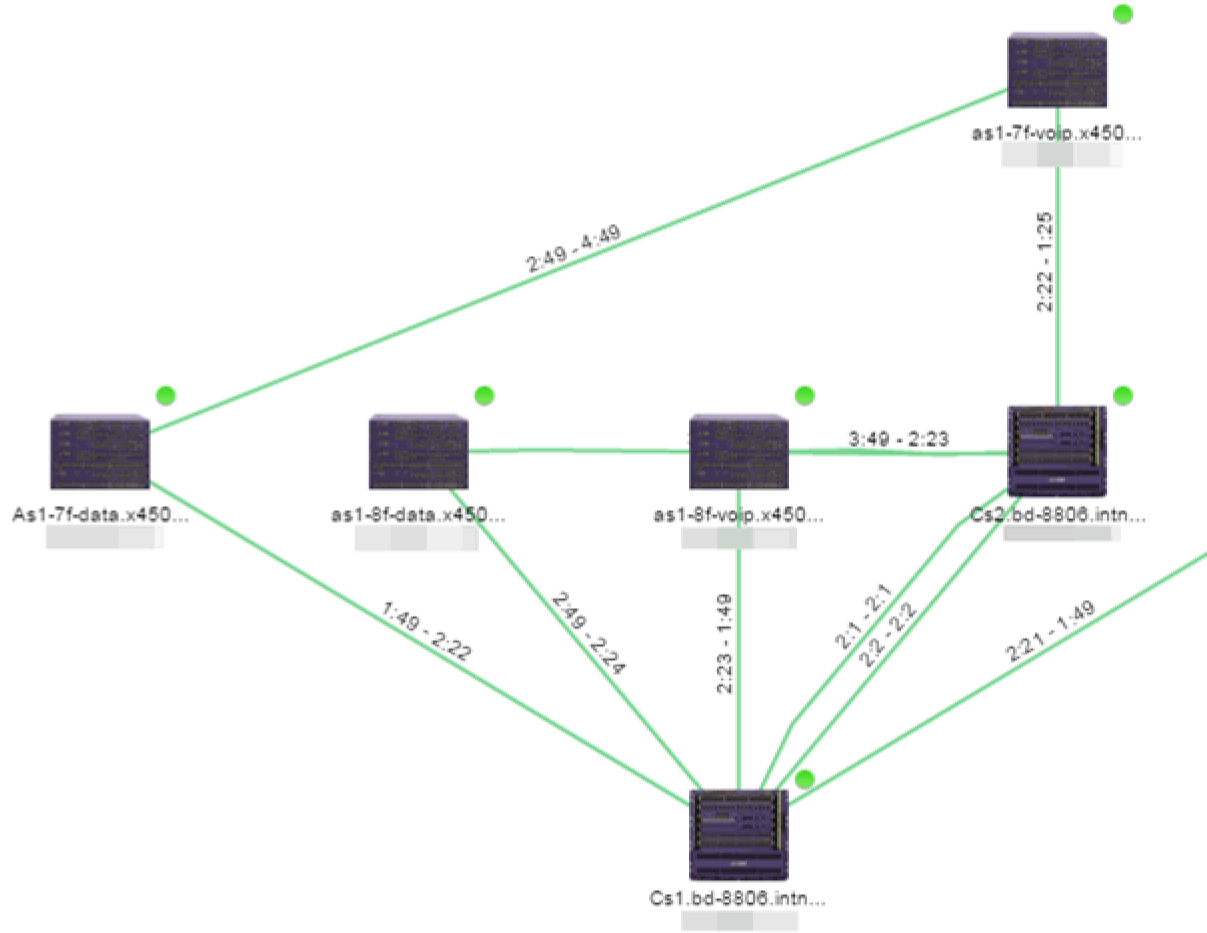
Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

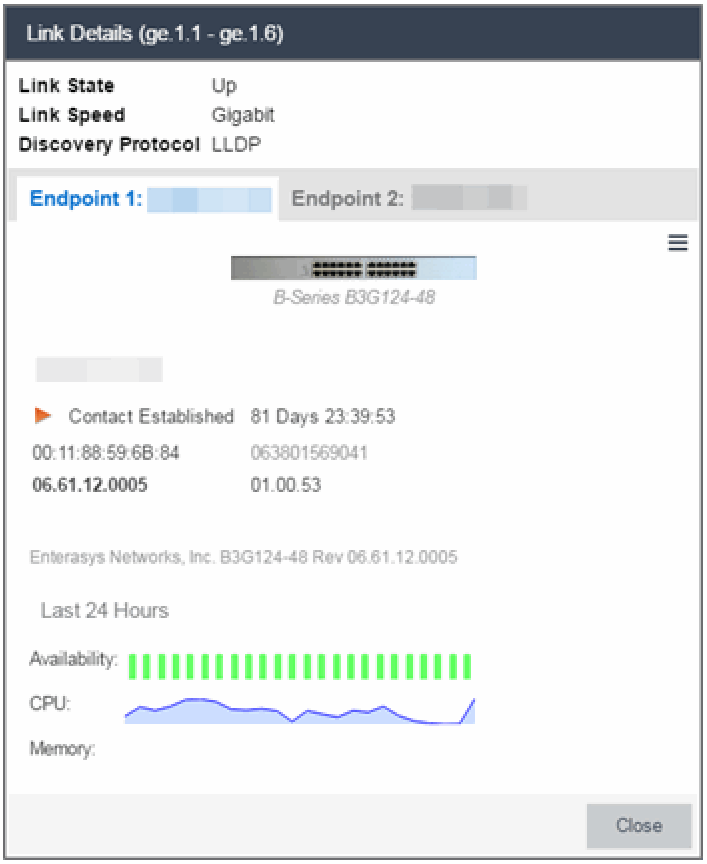
a. In the **Map Name** field, change the name for the map, if necessary.

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.



Link Details (ge.1.1 - ge.1.6)

Link State	Up
Link Speed	Gigabit
Discovery Protocol	LLDP

Endpoint 1: [redacted] **Endpoint 2:** [redacted]

B-Series B3G124-48

[redacted]

Contact Established	81 Days 23:39:53
00:11:88:59:6B:84	063801569041
06.61.12.0005	01.00.53

Enterasys Networks, Inc. B3G124-48 Rev 06.61.12.0005

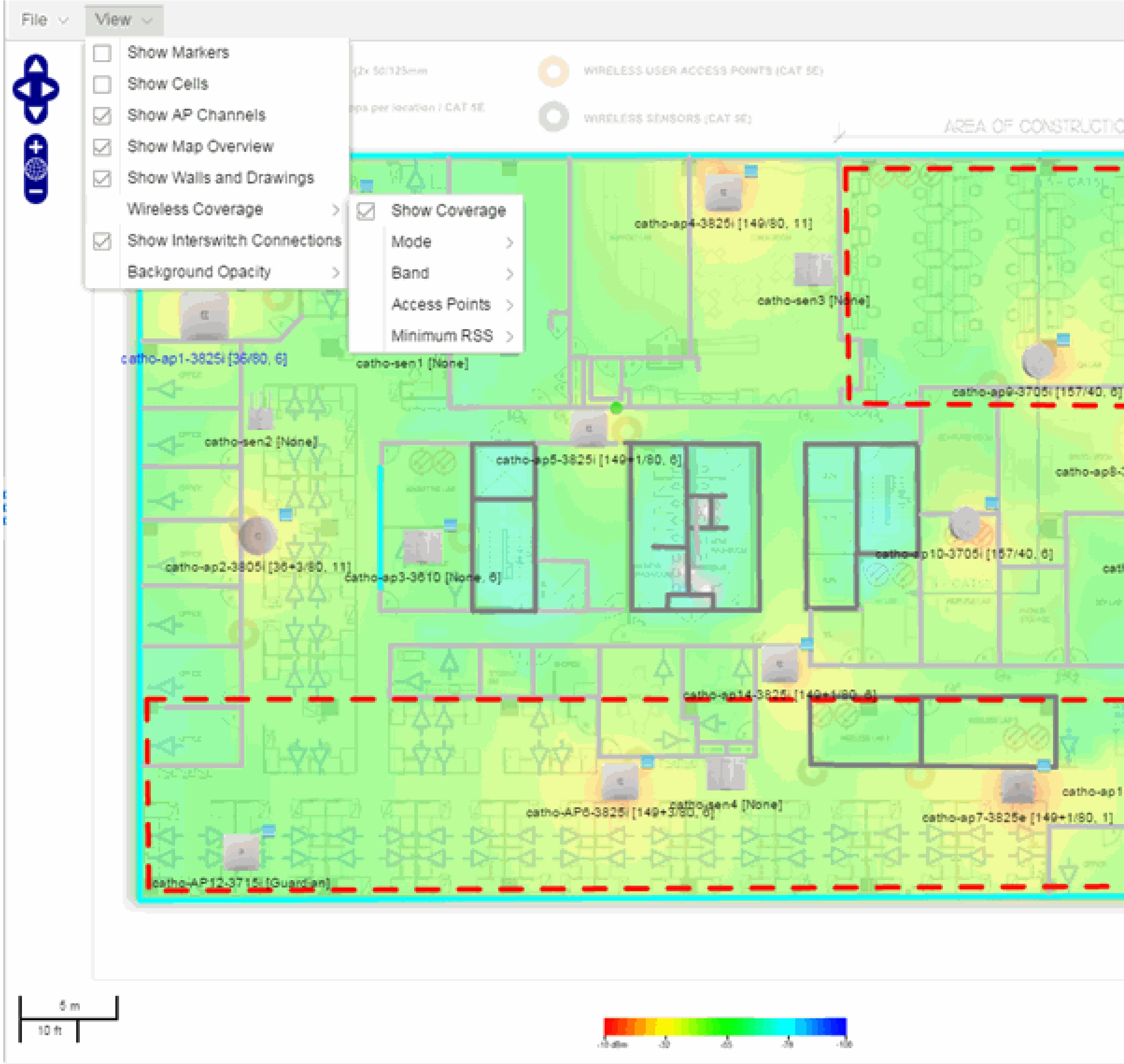
Last 24 Hours

- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in .png, .gif, and .jpg formats. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed.

  If you select this option, a Map Image field displays under the Map Type field. In the Map Image field, use the drop-down menu to select an image or click the ⊕ button to open a window where you can select a local image and upload it to the Extreme Management Center server.

CAUTION: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage
☑ Show Interswitch Connections
Background Opacity
☑ Show Coverage
Mode
Band
Access Points
Minimum RSS
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTIO
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap7-3825e [149+1/80, 1]
catho-ap1
catho-AP12-3715i [Guardian]
5 m
10 ft

If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located.

If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located. For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the

AP's radio frequencies are not being obstructed by any walls, and the area where a client might be located is larger.

- Open space — The wireless APs are located in an environment with no walls or cubicles.
- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — For customers with a NMS-ADV license, use this option to create custom floorplans.

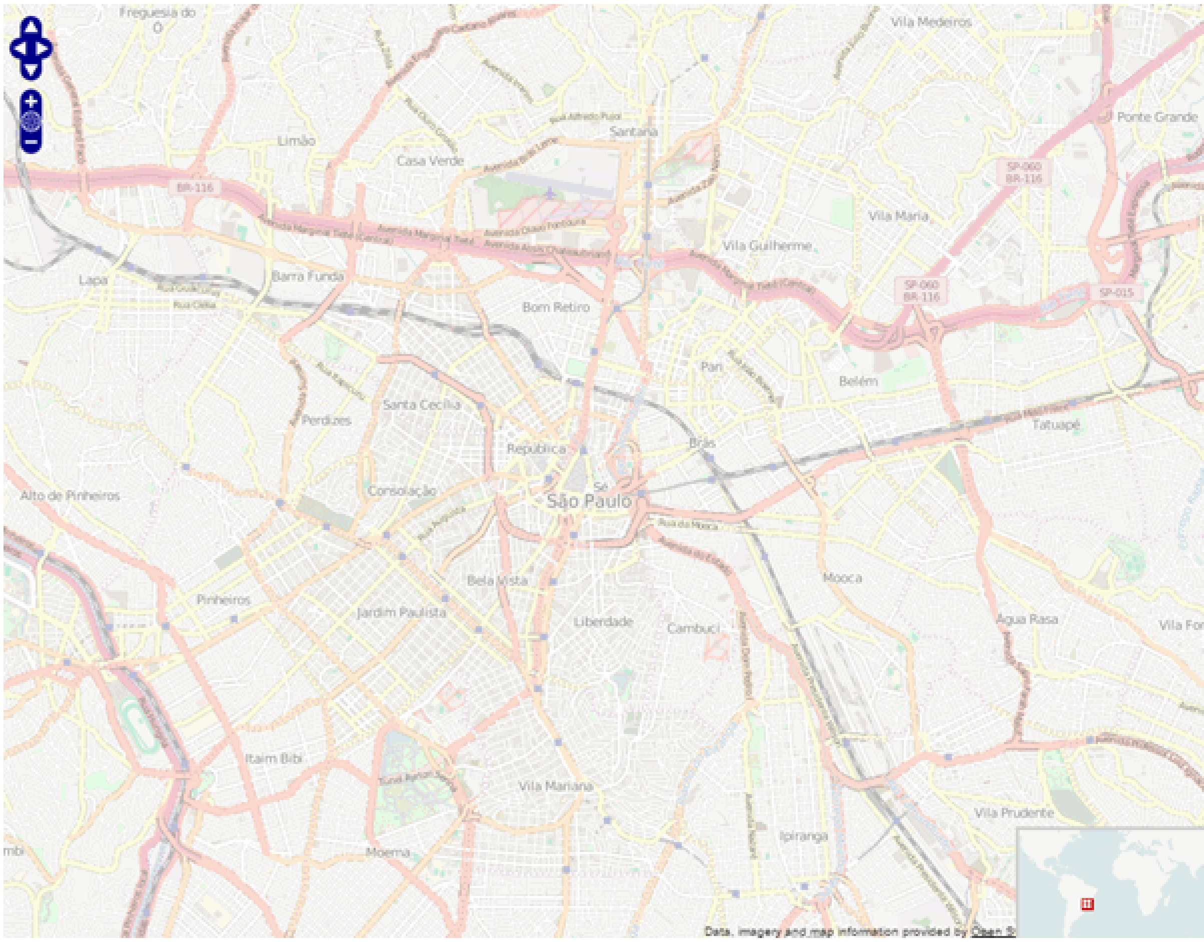
An additional Floor Plan option is available for users with the Extreme Management Center NMS-ADV license.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down menu to select an image or click **Add** (⊕) to open a window where you can select a local image and upload it to the Extreme Management Center server.

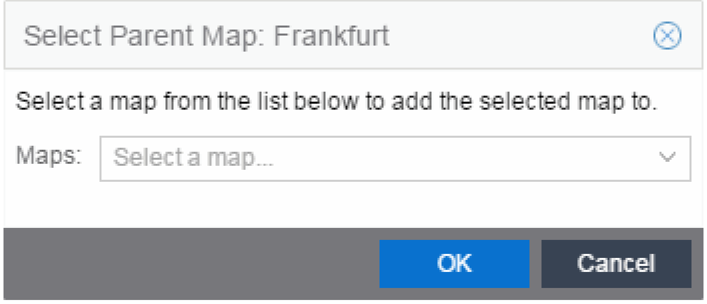
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Geographic — Displays a global or regional map where network locations are shown geographically.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



Select Parent Map: Frankfurt ⊗

Select a map from the list below to add the selected map to.

Maps: Select a map...

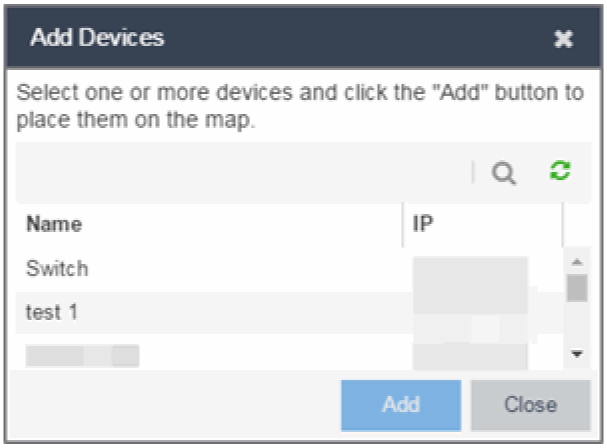
d. Click **Save**.

e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like world or city maps. For example, if a person viewing a map changes the location and zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.

The Pan control allows you to move left/right and up/down in the map.

The Zoom control lets you zoom in and out of the map.

4. Add your devices, APs, or Links to the map you are currently editing by clicking **File** > **Add** > **Devices/APs/Map Link**. This opens the Add window.



Add Devices

Select one or more devices and click the "Add" button to place them on the map.

Name	IP
Switch	
test 1	

Use the **Search** icon to locate a specific device or AP in the Add Device or Add AP windows, respectively, or select another Map to which to link from the drop-down menu in the Add Link To Map window. Click the **Add** button to add the device, AP, or link to your network map.

5. Once your devices and/or APs are located on your map, manually manipulate the devices, APs, and links on the map, or organize them automatically by clicking **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
   - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.
   - Hierarchical — Organizes devices, APs, and links in a tree pattern.
   - Circular — Organizes devices, APs, and links in a circular pattern.
6. Click **File** > **Save** button to save the map.

NOTE: Map devices and APs do not show their current status until you save the map.

7. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or click the **Edit** button in the Map Properties panel.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Edit Maps

The Extreme Management Center Maps feature lets you edit newly created maps of the devices and wireless access points (APs) on your network.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

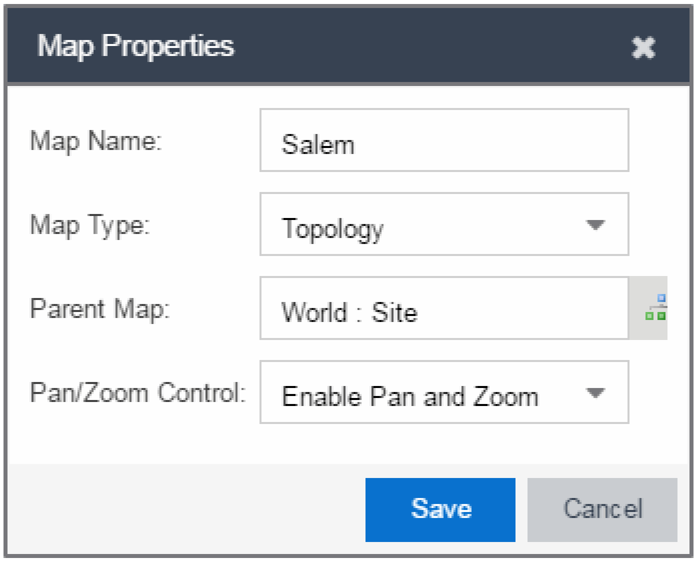
Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Editing a Map

To edit a new Device map properties:

1. Select a new map from the left-panel. The new map is initially blank unless you create it from a device or AP by selecting the device or AP, clicking the **Menu** icon (≡) or right-clicking the device or AP and selecting **Maps** > **Create Map**.
2. Click **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



Map Name: Salem

Map Type: Topology

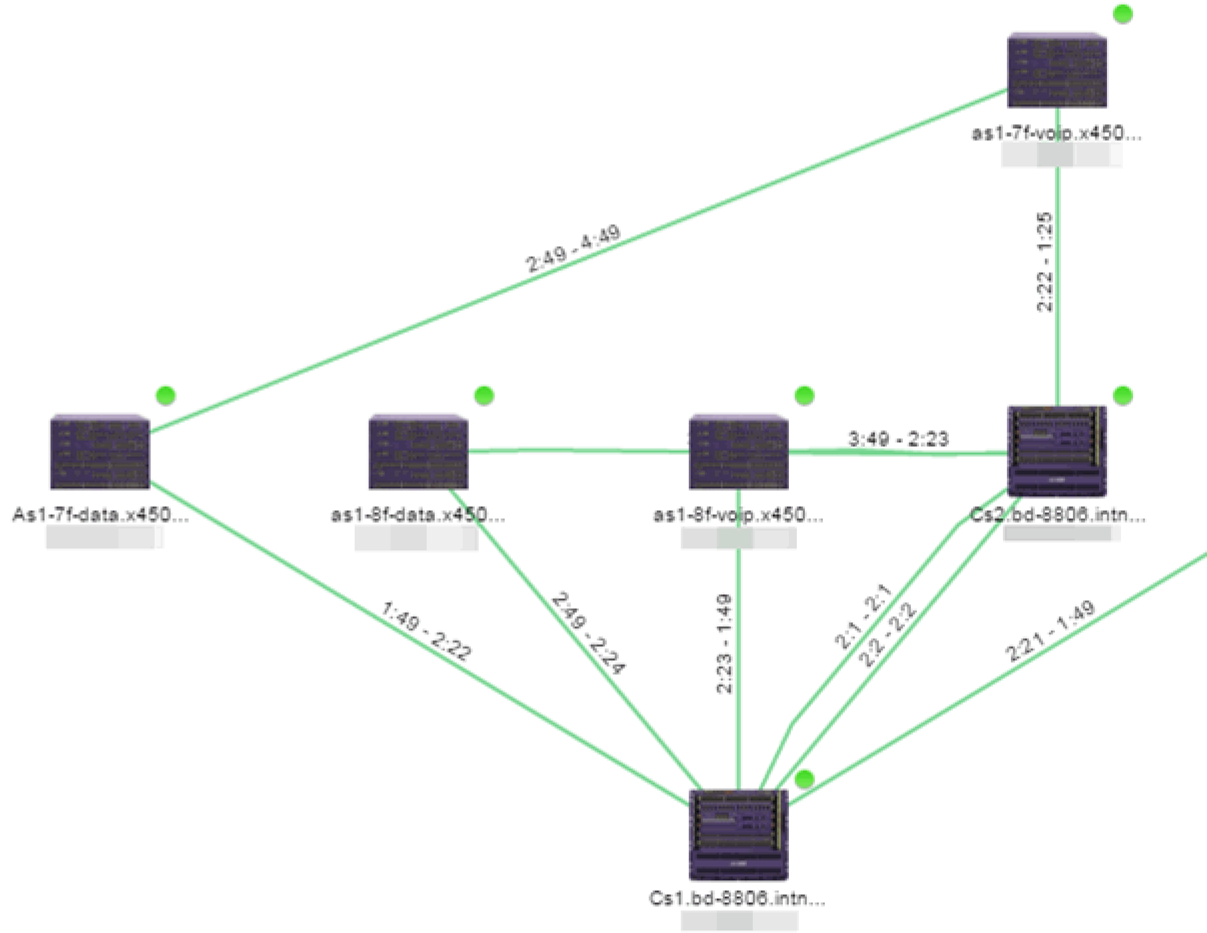
Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

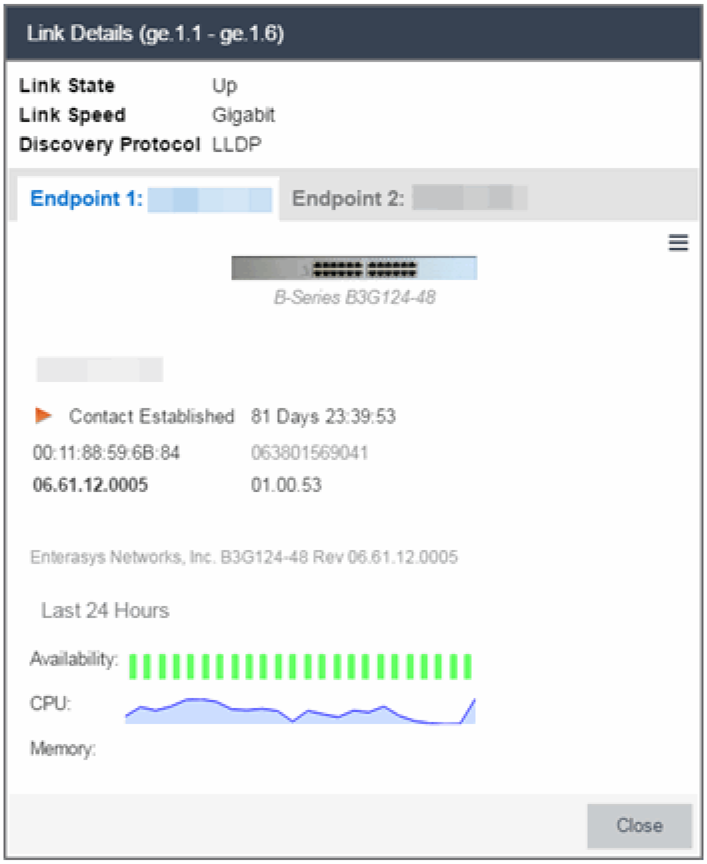
a. In the **Map Name** field, change the name for the map, if necessary.

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.



Link Details (ge.1.1 - ge.1.6)

Link State Up
Link Speed Gigabit
Discovery Protocol LLDP

Contact Established 81 Days 23:39:53
00:11:88:59:6B:84 063801569041
06.61.12.0005 01.00.53

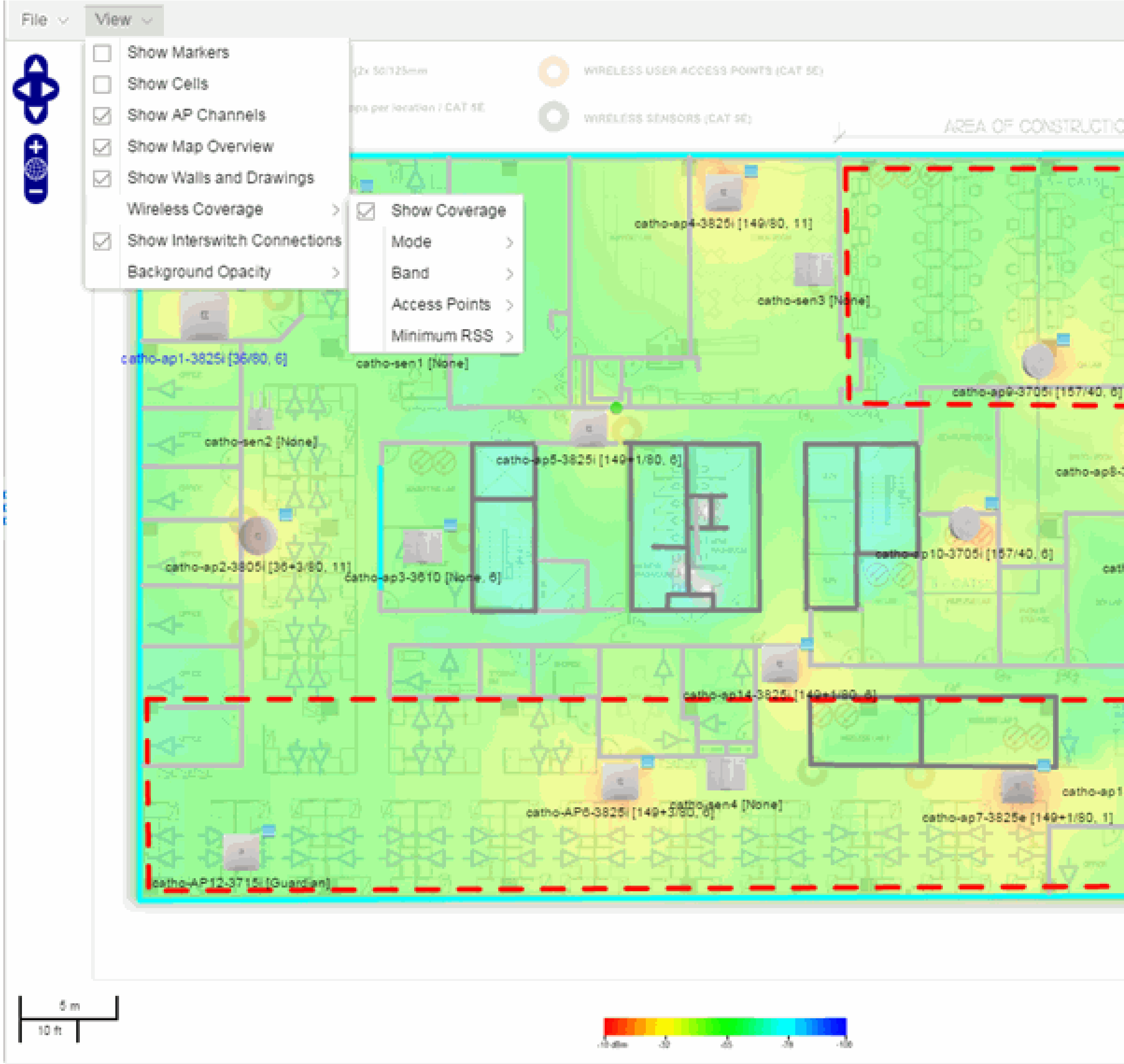
Enterasys Networks, Inc. B3G124-48 Rev 06.61.12.0005

- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in the .png, .gif, and .jpg format. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed.

  If you select this option, a **Map Image** field displays under the **Map Type** field. In the **Map Image** field, use the drop-down menu to select an image or click the ⊕ button to open a window where you can select a local image and upload it to the Extreme Management Center server.

  CAUTION: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage
☑ Show Interswitch Connections
Background Opacity
☑ Show Coverage
Mode
Band
Access Points
Minimum RSS
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTIO
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap7-3825e [149+1/80, 1]
catho-ap1
catho-AP12-3715i [Guardian]
5 m
10 ft

If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located.

If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located. For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the

AP's radio frequencies are not be obstructed by any walls, and the area where a client might be located is larger.

- Open space — The wireless APs are located in an environment with no walls or cubicles.
- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — For customers with a NMS-ADV license, use this option to create custom floorplans.

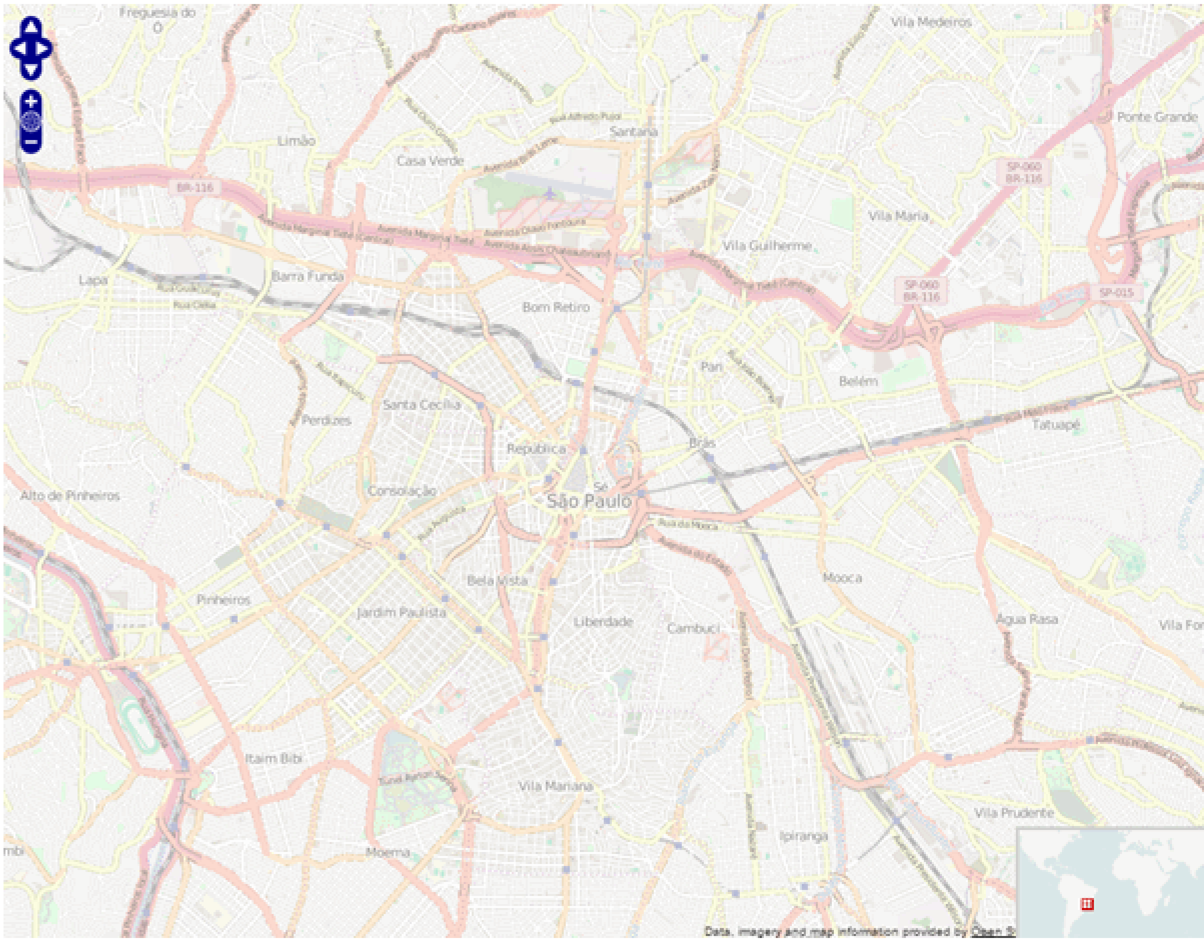
An additional Floor Plan option is available for users with the Extreme Management Center NMS-ADV license.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down menu to select an image or click **Add** (⊕) to open a window where you can select a local image and upload it to the Extreme Management Center server.

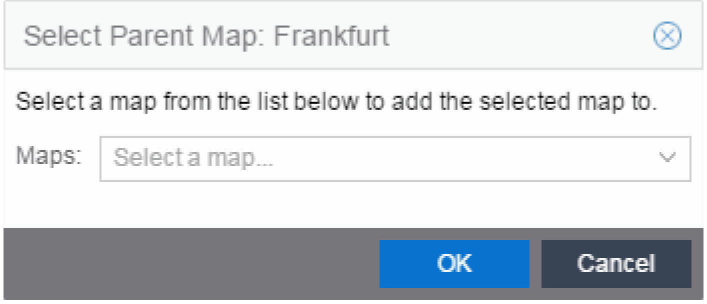
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Geographic — Displays a global or regional map where network locations are shown geographically.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



Select Parent Map: Frankfurt

Select a map from the list below to add the selected map to.

Maps: Select a map...

d. Click **Save**.

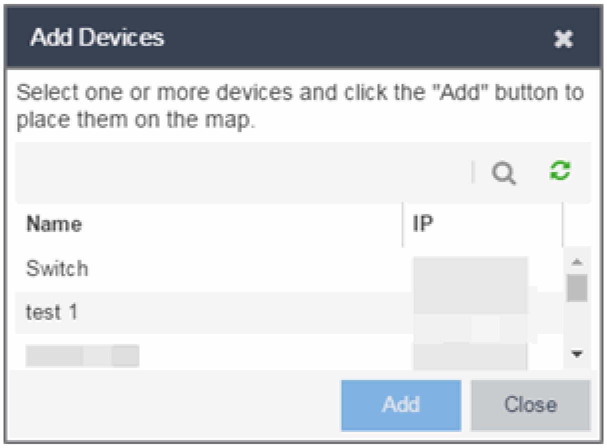
e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like world or city maps. For example, if a person viewing a map changes the location and zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.

The Pan control allows you to move left/right and up/down in the map.

The Zoom control lets you zoom in and out of the map.

Adding Devices, APs and Links to a Map

1. Click **File** > **Add** > **Devices/APs/Map Link** to add your devices, APs, or Links to the map you are currently editing. This opens the Add window.



Add Devices

Select one or more devices and click the "Add" button to place them on the map.

Name	IP
Switch	[redacted]
test 1	[redacted]
[redacted]	[redacted]

2. Use the **Search** icon to locate a specific device or AP in the Add Device or Add AP windows, respectively, or select another Map to which to link from the drop-down menu in the Add Link To Map window. Click the **Add** button to add the device, AP, or link to your network map.
3. Once your devices and/or APs are located on your map, manually manipulate the devices, APs, and links on the map, or organize them automatically by clicking **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
   - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.

  - Hierarchical — Organizes devices, APs, and links in a tree pattern.
  - Circular — Organizes devices, APs, and links in a circular pattern.

4. Click **File** > **Save** button to save the map.

   NOTE: Map devices and APs do not show their current status until you save the map.

5. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or click the **Edit** button in the Map Properties panel.

Related Information

- Extreme Management Center Maps
  - Types of Maps
  - Navigate Map Tab
    - Network Details Overview
    - EAPS Summary Tab
    - Link Summary Tab
    - VLAN Summary Tab
    - MLAG Summary Tab
    - VPLS Summary Tab
  - Search Maps
  - Create Maps
  - Add Devices or APs to Maps
  - Add Links Between Devices and Maps
  - Import Maps
  - Export Maps
  - Set Map Scale
- Advanced Map Overview
  - Design Map Floorplans
  - Display Map Application Data

- Locate Wireless Clients
- View Wireless Coverage

Advanced Map Features Overview

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) include custom floor plan design, triangulated wireless client location, and wireless coverage maps to identify coverage trouble spots for your wireless network.

Overview

Extreme Management Center advanced Map features provide the following enhanced functionality:

- **Detailed Floor Plans** — Advanced map functionality lets you create detailed floor plans for both your wired and wireless networks. Using floor plans provides greater accuracy in calculations of wireless client location and displays wireless device coverage. You can upload and modify existing floor plans or create new floor plans from scratch. Use the Map drawing tools and menus to specify wall types, material, and thickness and then configure AP locations, type, and orientation.
- **Wireless Location** — Advanced location (triangulation) enhances client location results, improving visibility when investigating wireless trouble spots. Colored distribution displays high, medium, and low confidence locations, with the client icon displayed in the highest confidence location. Using floor plan data, a single client's location is triangulated based on the client's contact with multiple access points in the covered area. The floor plan wall type information helps determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls. This helps define the probable distance of a client from a given access point. You need at least three access points to report triangulated location. You can also view time-lapse location coverage for a client, using historic triangulated location results.
- **Wireless Coverage** — This feature provide a graphical view of wireless coverage, allowing quick identification of possible coverage trouble spots. Wireless coverage is displayed using different colors to indicate radio signal strength based on the

distance from access points included on the map. Coverage is determined by computing the approximate radio signal strength at fixed distances from access points, with floor plan and wall information used to provide accuracy in the signal strength computation.

- Import and Export Maps — The map import function gives you the ability to import Ekahau maps into floor plan maps. This function also lets you export floor plan maps to a ZIP file.
- Show Application Data in Maps — Use map links tied to Application Analytics network locations to display network application flow data in a map.

Prerequisites

Review the following prerequisites for using the Extreme Management Center advanced Map features:

- To access the advanced Map features, the Extreme Management Center server must be running version 6.2 with a Extreme Management Center (NetSight) Advanced license (NMS-ADV).
- In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software User Guide.*)
- The Access Points must be model 37xx, 38xx, or 39xx.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Advanced Map Features

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) include custom floorplan design, triangulated wireless client location, and wireless coverage maps to identify coverage trouble spots for your wireless network.

This Help topic provides the following information:

- Overview of Advanced Map Features
- Prerequisites
- Designing a Floorplan
    - Drawing Tools
    - Configure Area Window
    - Style Menu
- Wireless Client Location
    - Time-Lapse Location
- Wireless Coverage
- Import and Export Maps
    - Importing Maps
    - Exporting Maps
- Show Application Data
    - Adding a Map Link with Location
- Wireless Map Limits

For information on viewing and searching maps, see View and Search Maps.

Overview

Extreme Management Center advanced Map features provide the following enhanced functionality:

- Detailed Floorplans — Advanced map functionality lets you create detailed floorplans for both your wired and wireless networks. Using floorplans provides greater accuracy in calculations of wireless client location and displays wireless device coverage. You can upload and modify existing floorplans or create new floorplans from scratch. Use the Map drawing tools and menus to specify wall types, material, and thickness and then configure AP locations, type, and orientation.
- Wireless Location — Advanced location (triangulation) enhances client location results, improving visibility when investigating wireless trouble spots. Colored distribution displays high, medium, and low confidence locations, with the client icon displayed in the highest confidence location. Using floorplan data, a single client's location is triangulated based on the client's contact with multiple access points in the covered area. The floorplan wall type information helps determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls. This helps define the probable distance of a client from a given access point. You need at least three access points to report triangulated location. You can also view time-lapse location coverage for a client, using historic triangulated location results.
- Wireless Coverage — This feature provide a graphical view of wireless coverage, allowing quick identification of possible coverage trouble spots. Wireless coverage is displayed using different colors to indicate radio signal strength based on the distance from access points included on the map. Coverage is determined by computing the approximate radio signal strength at fixed distances from access points, with floorplan and wall information used to provide accuracy in the signal strength computation.
- Import and Export Maps — The map import function gives you the ability to import Ekahau maps into floorplan maps. This function also lets you export floorplan maps to a ZIP file.
- Show Application Data in Maps — Use map links tied to Application Analytics network locations to display network application flow data in a map.

Prerequisites

Review the following prerequisites for using the Extreme Management Center advanced Map features:

- To access the advanced Map features, the Extreme Management Center server must be running version 6.2 with a Extreme Management Center (NetSight) Advanced license (NMS-ADV).

- In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software User Guide.*)
- The Access Points must be model 37xx, 38xx, or 39xx.

Designing a floorplan

You can design and enhance floorplans of your wired and wireless network environment by editing your maps using the drawing and style tools. These editing tools allow you to create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

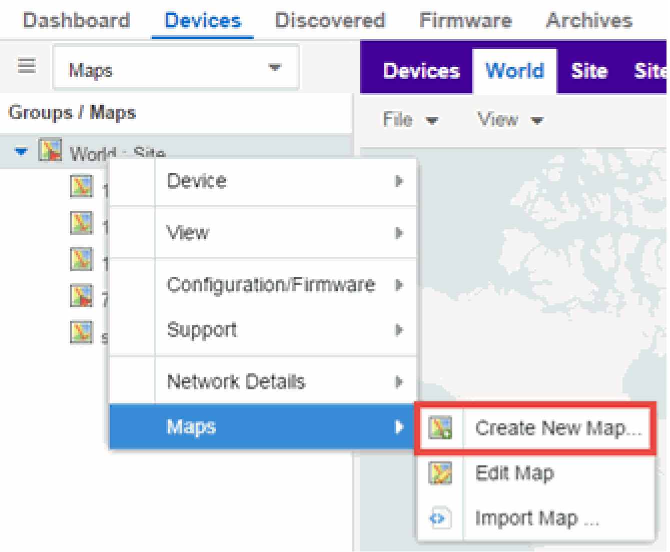
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

A floorplan can be created with or without a reference background image, however it is much easier to use the drawing features with an existing image. (The Map feature supports images in the .png, .gif, and .jpg formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thickness, and wall color to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provide greater accuracy in wireless calculations.

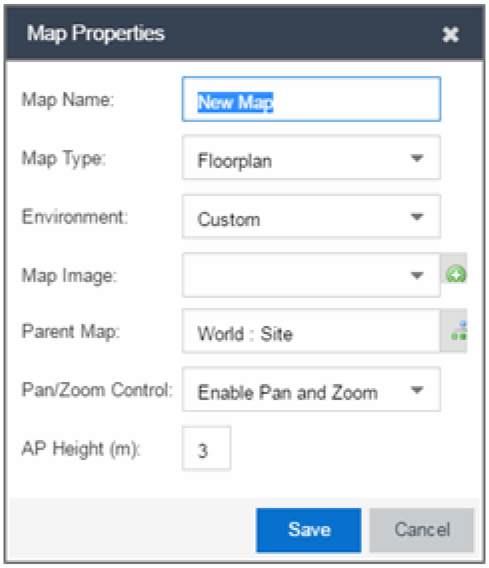
1. Create and configure a new map.
   a. Launch Extreme Management Center and click on the **Network** > **Devices** tab.
   b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



Map Properties

Map Name: New Map

Map Type: Floorplan

Environment: Custom

Map Image:

Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

AP Height (m): 3

e. Change the **Map Type** drop-down menu to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in the .png, .gif, and .jpg formats. The maximum image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

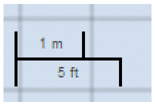
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

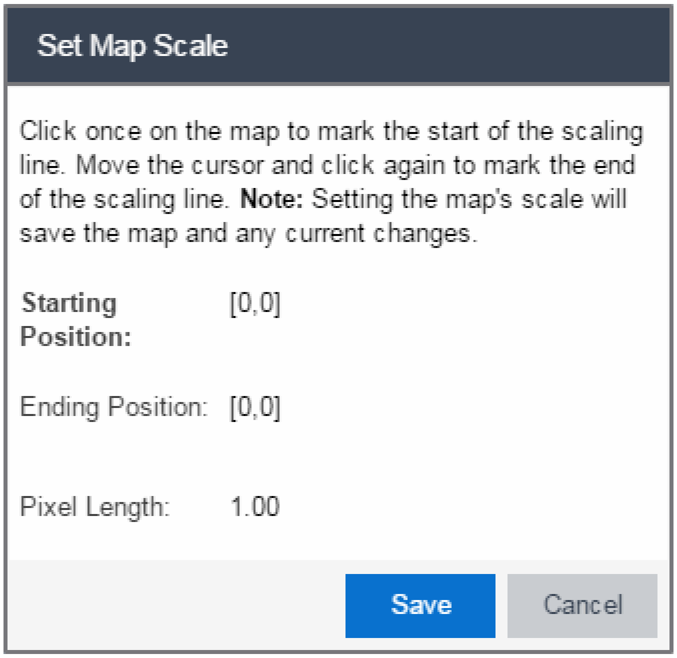
i. Click **Save** to save the map and display the image.

2. **Set the map scale.** It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Click **File** > **Edit** to open the map in edit mode.

   b. Click on the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)




Set Map Scale

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. **Note:** Setting the map's scale will save the map and any current changes.

Starting Position: [0,0]

Ending Position: [0,0]

Pixel Length: 1.00

c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

   i. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.

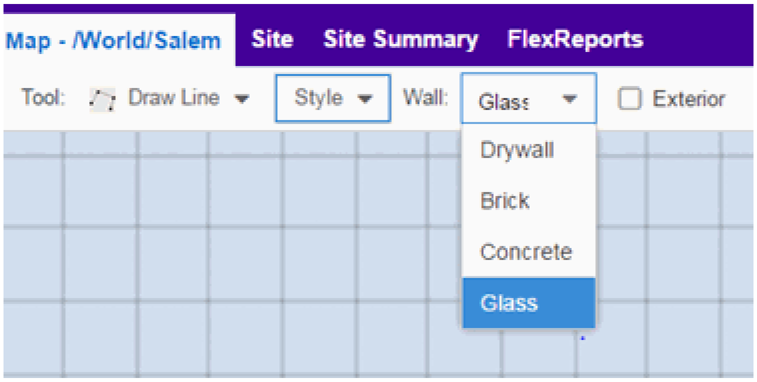
   ii. Enter the line length and units.

d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

   b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down menu and select the checkbox to specify that the wall is an exterior wall.



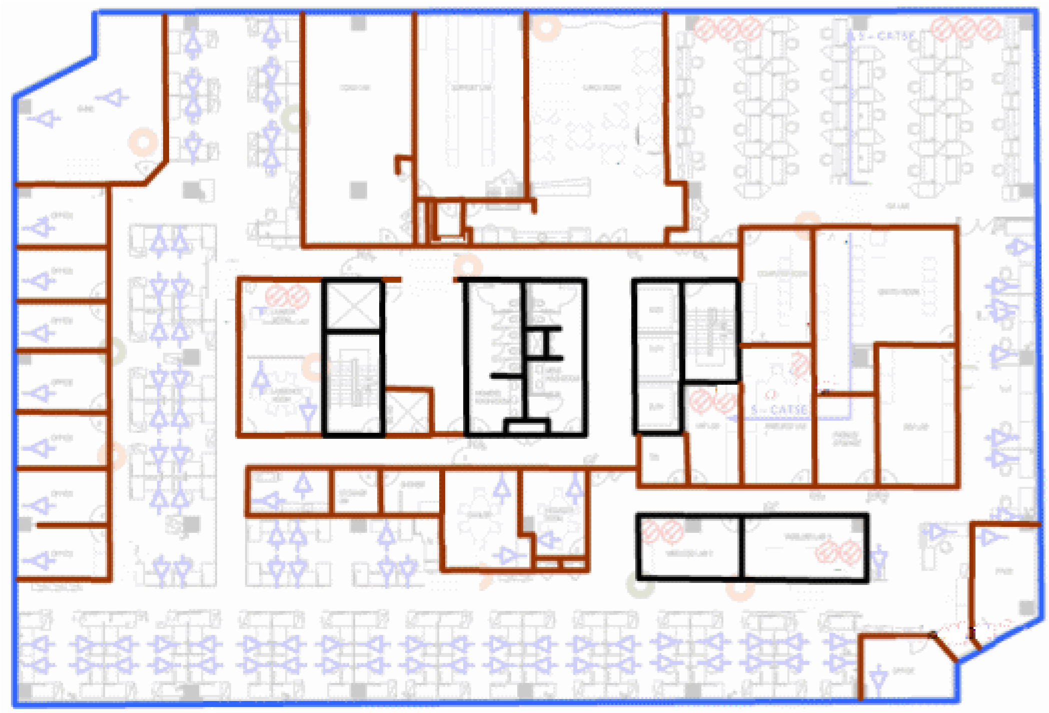
   c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

   d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

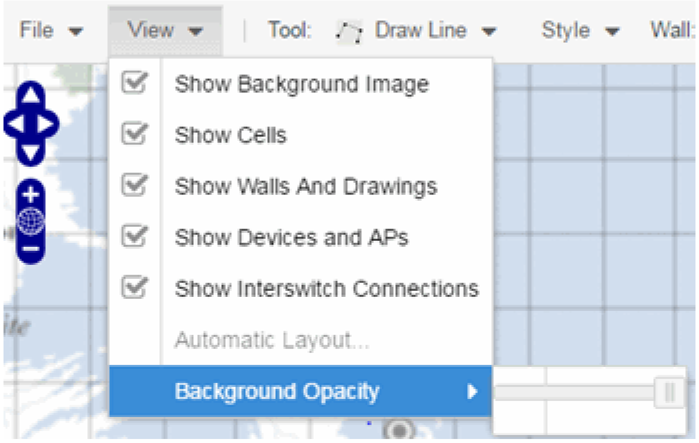
   You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, click **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



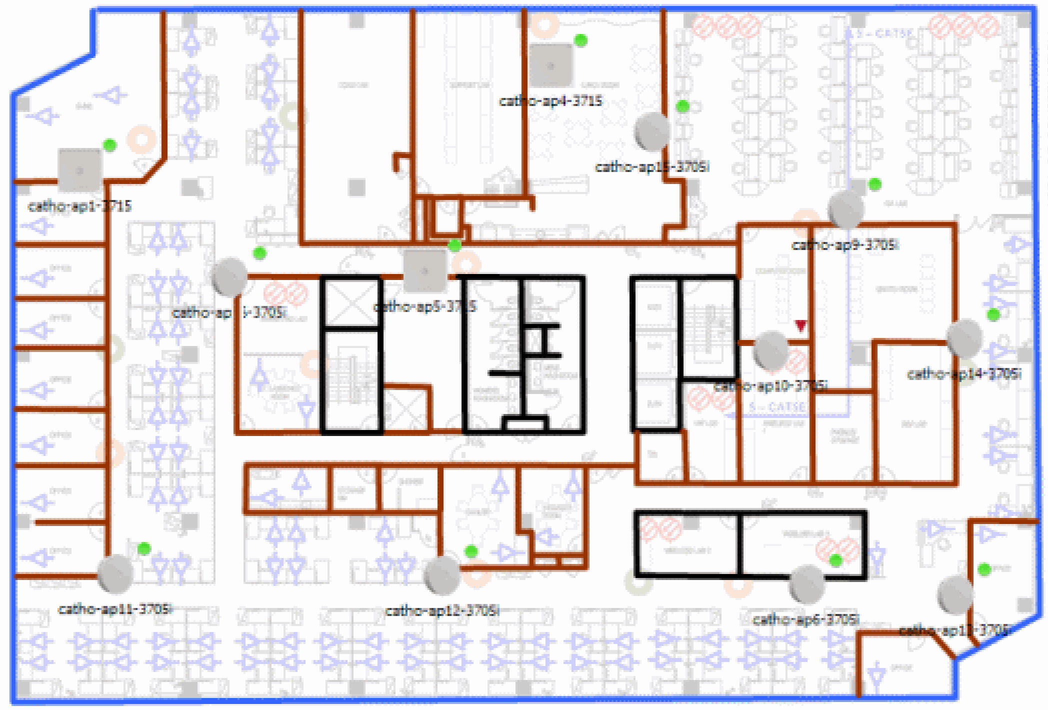
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can use the search field to locate a specific device or AP.

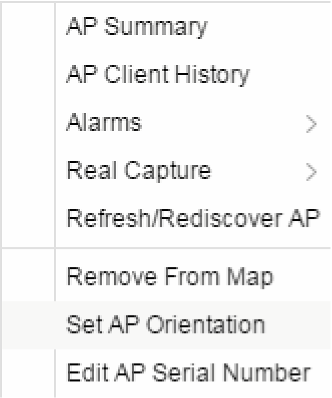
   Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the

AP. Be sure to place an AP on the correct side of a wall.

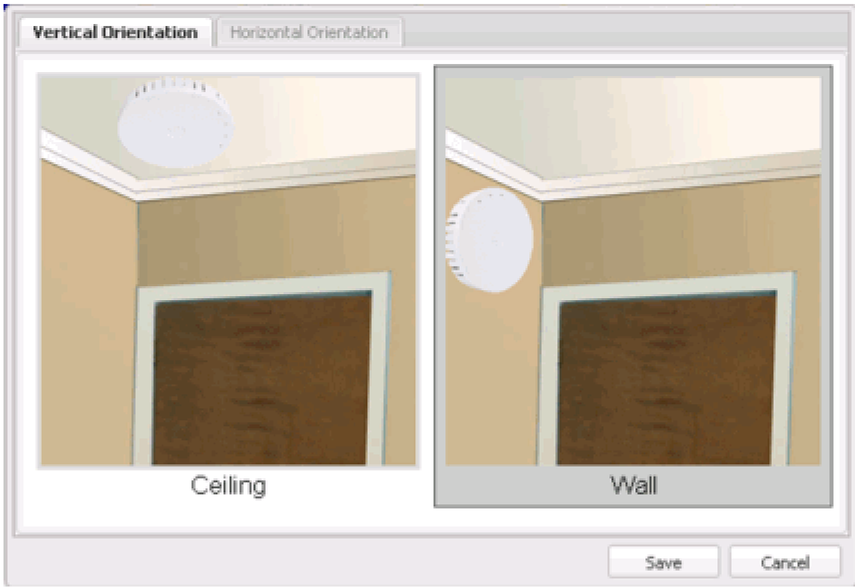


5. Set AP orientation.

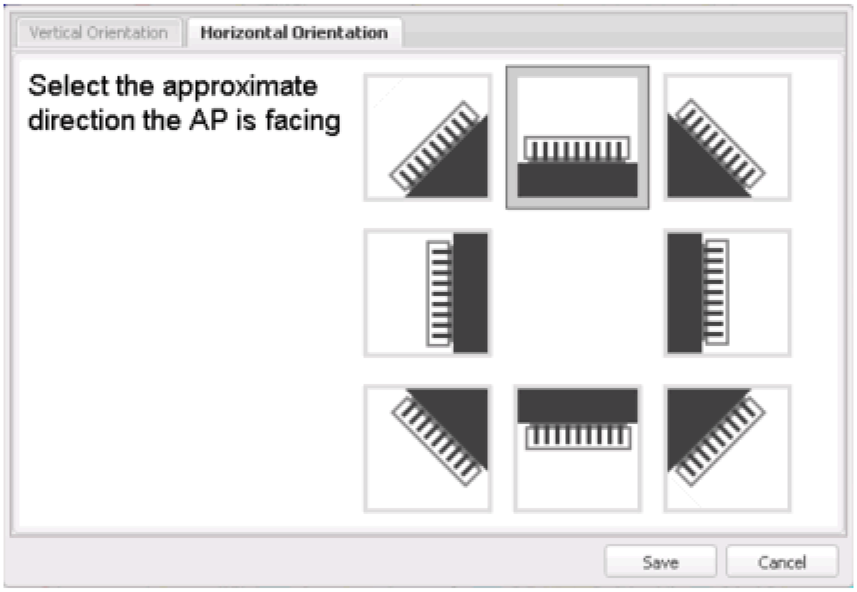
   a. Right-click on an AP in the map and select **Set AP Orientation**.



   b. Click on the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.



c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



Select the approximate direction the AP is facing

d. Click **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.

Over AP
Orientation: Wall facing east

6. Click **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and coverage information. See the sections on wireless location and wireless coverage.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down menu to specify whether to:
    - Display markers instead of device images on your map
    - Display cells on the map image to show the map's actual image area
    - Display AP channel information (if available)
    - Display walls and drawings
    - Show application data for map links (if available)
    - Set the map's background opacity
    - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the **Tool** menu.

Drawing Tool	Definition
✋	Select Items Click on a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Click anywhere on the map and drag to reposition the map image.

Drawing Tool	Definition
⬠	Draw Area Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
⬠	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.
□	Draw Rectangle Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
✎	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click to add the text to your map. Use the **Style** menu to change the text appearance.
△	Draw Triangle Position the cursor where you want the triangle. Click and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
╱	Draw Line Position your cursor where you want to start drawing the line. Click once and draw the line. Click to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.

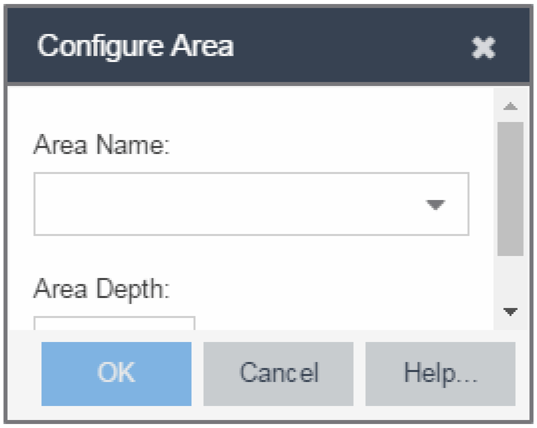
Drawing Tool	Definition
⟳	Rotate Shape Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
⬚	Set Scale Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

> **NOTE:** The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

Wireless Client Location

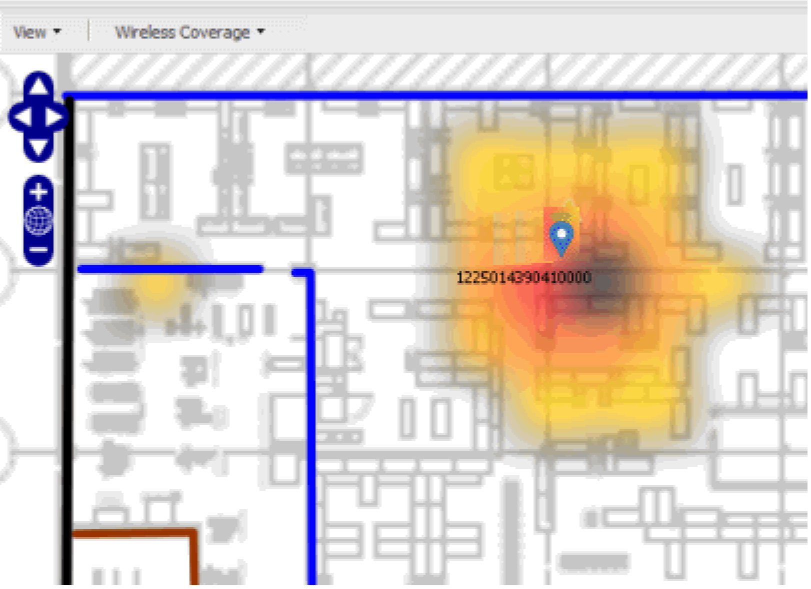
The wireless location feature requires you enable the location engine on the wireless controller. Once you add APs to your custom floorplan and save the map, a copy of the floorplan is sent to each controller. The location engine incorporates information defined in the floorplan data and signal information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to determine a client's triangulated location.

To search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map **Search** box and press **Enter**. (The client must be connected to an AP added to a map.)

The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence. You can use the **Min. Location Confidence** slider on the **View** menu to filter out lower confidence colors. As you drag the slider, colors below the selected confidence level are no longer displayed. If you set the slider to the right-most point, only black is displayed.

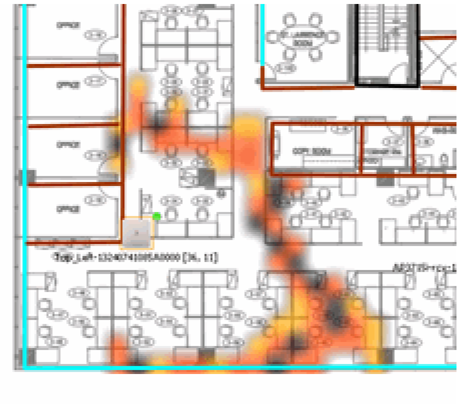
Mouse over the client icon to see a tooltip with client information.

NOTE: The tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the **Wireless** > **Clients** tab and the confidence colors are not displayed.

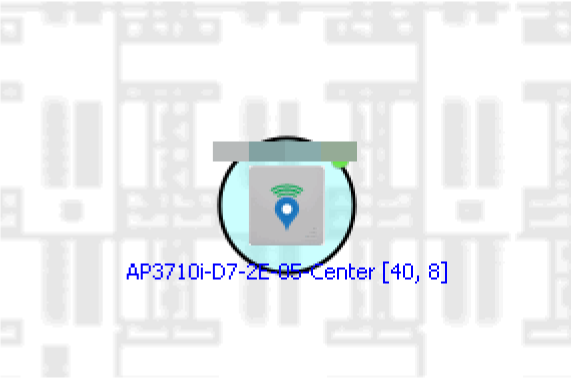


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.



If there is insufficient data to provide triangulated results, the map displays the AP in the center, with a circle showing the possible area where the client may be located, based on the client's RSS (Received Signal Strength).



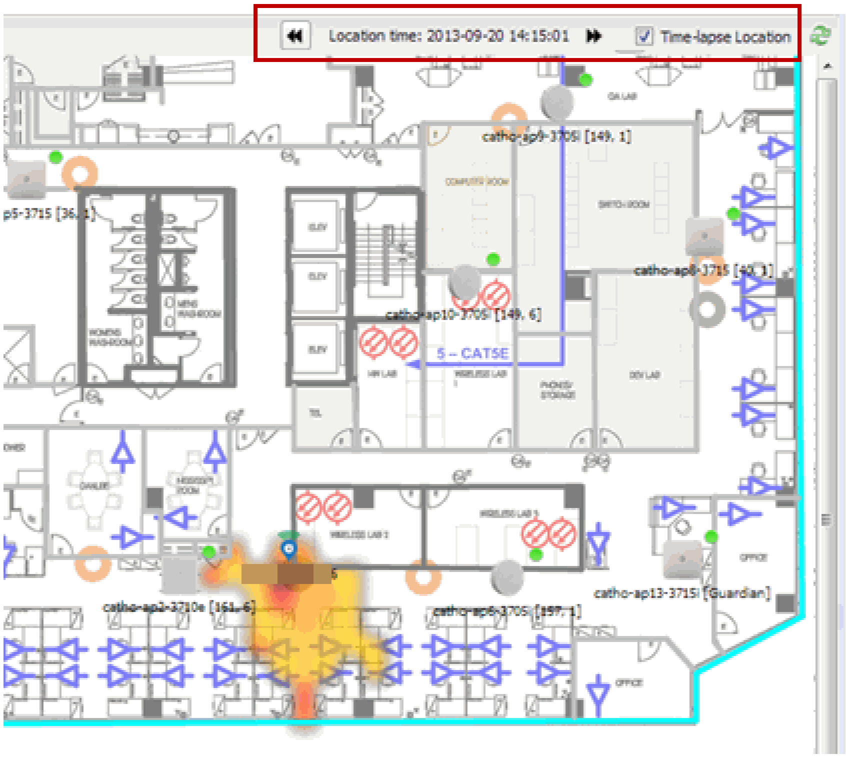
Time-Lapse Location

The wireless location feature provides the ability to view time-lapse location coverage for a client, using historic triangulated location results. This allows you to understand a wireless client's movement through the network and provides for better network troubleshooting.

When a current triangulated location search result displays, a checkbox is available in the upper right corner to enable time-lapse location.

When the checkbox is selected, a set of controls appears to the left of the checkbox, indicating the date of the displayed result. If there are historic events available, the Rewind arrow is enabled and you can scroll through the history. Note that for a historic location, the client icon displays a small clock inside it.

The Rewind and Fast-Forward arrows are disabled if there is no more history in that direction. After viewing historic locations, if you fast forward to the current location and it changed, the location updates.



Wireless Coverage

After you finish your custom floorplan and saved the map, the map is ready to display wireless coverage information. Select View > Wireless Coverage > Show Coverage to show wireless coverage of the APs on the map and to enable the wireless coverage options. Use the View > Wireless Coverage menu available at the top of the map to select from the following coverage display options.

- Mode — Select from the different options for coverage display:
  - Signal Strength— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
  - Channel Coverage — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This mode provides a graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.

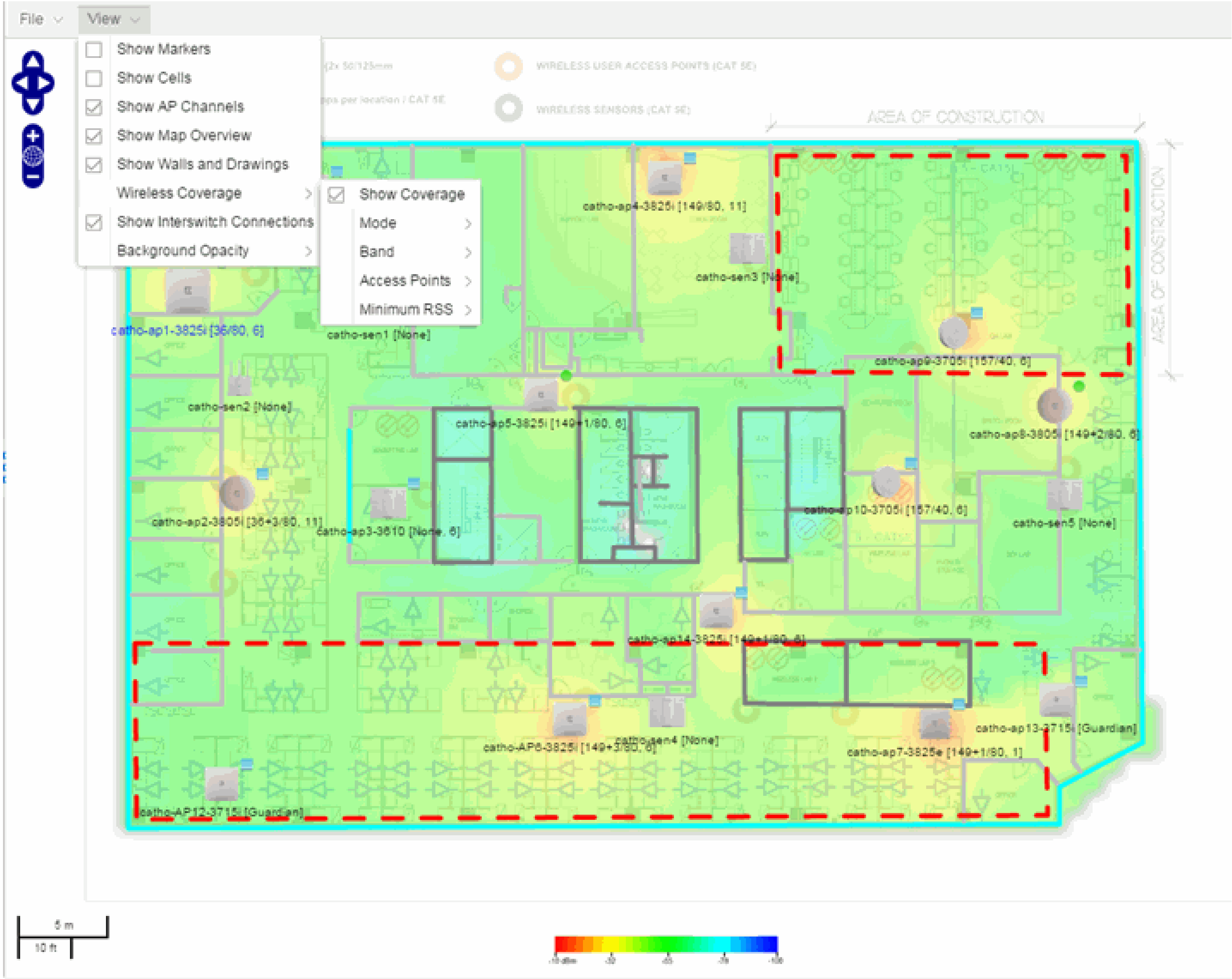
  - **Data Rate** — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and Access Points options. Use this mode to ensure proper wireless performance throughout the network.

NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

  - **Location Readiness** — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
    - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
    - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
    - Orange — Poor readiness. There are less than three APs with visibility of the cell.
    - Red — No triangulation. Only Cell of Origin location results are available in this area.
- **Select Channel** — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
  - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission of other stations or APs. This is an indicator of the congestion and interference on the channel.
  - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.
- **Min. Physical Rate** — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- **Band** — Select the desired band (radio frequency).

- Access Points — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- Minimum RSS — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

Once these options are set, the map displays the selected coverage information. The following map shows signal strength coverage.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage
☑ Show Interswitch Connections
Background Opacity
☑ Show Coverage
Mode
Band
Access Points
Minimum RSS
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTION
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-3805i [149+2/80, 6]
catho-ap10-3705i [157/40, 6]
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-sen5 [None]
catho-ap14-3825i [149+1/80, 6]
catho-ap13-3715i [Guardian]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap7-3825e [149+1/80, 1]
catho-AP12-3715i [Guardian]
5 m
10 ft
-10 dBm
-32
-55
-78
-100

Import and Export Maps

This section describes the map import and export functions. The map import function allows you to import Ekahau maps into Extreme Management Center floorplan maps. The map export function exports floorplan maps to a ZIP file.

Importing Maps

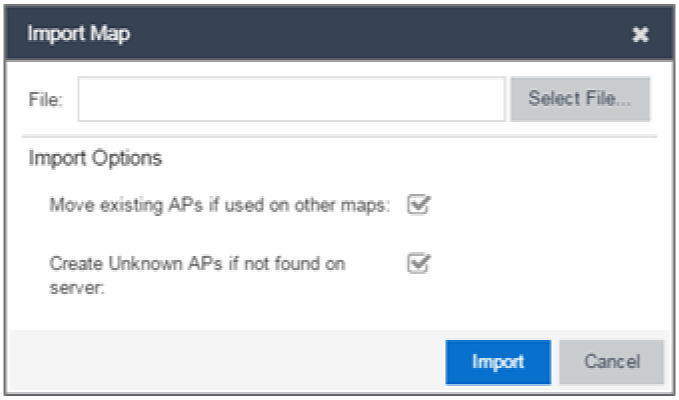
The map import function gives you the ability to import Ekahau maps into Extreme Management Center floorplan maps and gives you the ability to import floorplan maps are previously exported from Extreme Management Center maps.

When Ekahau maps are exported, all the maps in the system are combined into a single ZIP file. When the Ekahau ZIP file is imported into Extreme Management Center, each Ekahau map is re-created into an individual map again.

When a map is imported, it is added as a child map of the World map. If the map's name is not unique, a number is appended to the end of the name. After the map is imported it can be moved and renamed, if desired.

To import a map:

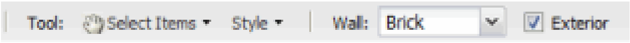
1. Launch Extreme Management Center and click on the **Network** > **Devices** tab.
2. In the left-panel, select Maps from the drop-down menu.
3. In the Groups/Maps navigation tree, right-click on the World map and select **Maps** > **Import Map**.
4. The Import Map window opens. Use the **Select File** button to navigate to the map file to import.



Move existing APs if used on other maps: ☑

Create Unknown APs if not found on server: ☑

5. Select the appropriate import options:
   - **Move existing APs if used on other maps** — An AP can only be added to a single map. If you select this option and import an AP that already exists on another map, the AP is moved from the existing map to the imported map.
   - **Create Unknown APs if not found on server** — If an AP is being imported that does not exist in Extreme Management Center, a placeholder AP is created. Once the map is imported, you can edit the placeholder and map it to an existing AP not currently in use on another map. To do this, right-click on the placeholder and select **Edit AP Serial Number**.
6. Click **Import**.
7. The map is imported and positioned under the World map. It can be moved and renamed, if desired.
8. All the walls in an Ekahau map are imported as internal walls. You need to manually edit the exterior walls after the floorplan is imported.
   a. Select the map and click **Edit** to edit the map.
   b. Click on the exterior wall and then select the **Exterior** checkbox. This designates the wall as an exterior wall.



Wall: Brick

☑ Exterior

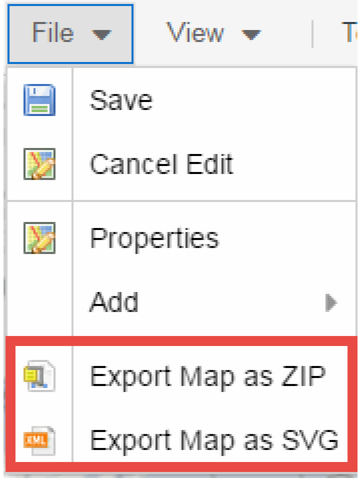
   c. Click **Save** to save the map.

Exporting Maps

The map export function gives you the ability to export floorplan maps as a ZIP or SVG file.

To export a map:

1. Launch Extreme Management Center and click on the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.
3. The map opens in Edit mode. Click **File** > **Export Map as ZIP** or **Export Map as SVG**.



- If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browsers default download location.
- If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

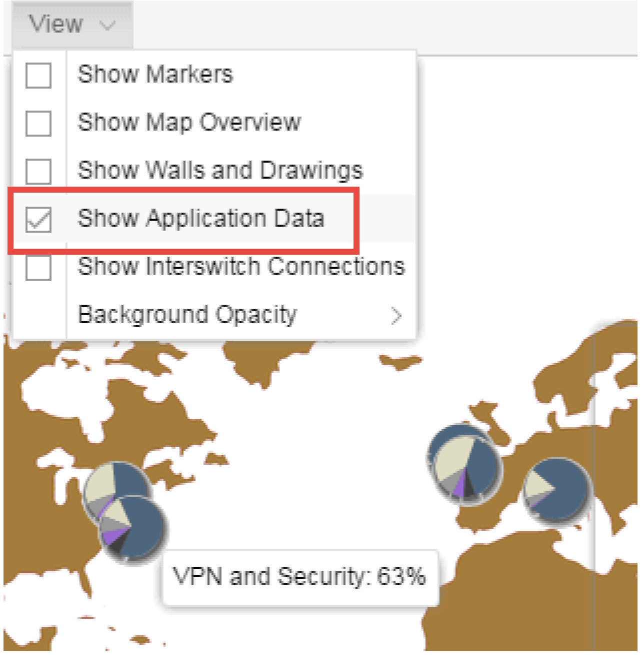
NOTE: The Export Map as ZIP option is only available for Floorplan map types.

Show Application Data

You can display application data in maps by creating map links tied to Application Analytics network locations. Application data for the location tied to the link displays in the map.

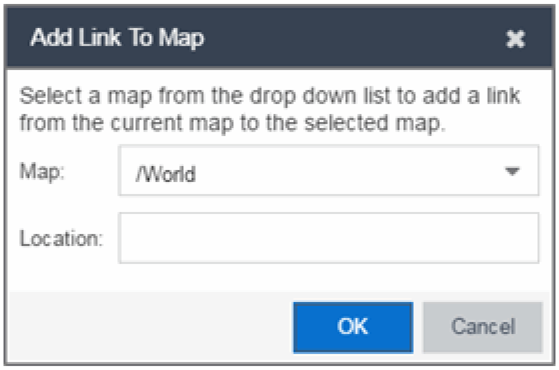
When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the Location field specified for the link and corresponds to a network location defined in the Application Analytics feature. For more information on network locations, see the section on Network Locations in the Application Analytics user guide.

The pie chart displays the top five application groups (by bytes transferred) for the location specified for the map link. Rest the cursor over the pie chart to view a tooltip. If there is no application data, nothing displays.



Adding a Map Link with Location

1. In the Maps navigation tree, right-click on the map you want to link from and select **Maps** > **Edit Map** or click **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Click **File** > **Add** > **Map Link**.
3. The Add Link to Map window opens.



Select a map from the drop down list to add a link from the current map to the selected map.

Map: /World

Location:

4. From the drop-down list, select the map to which you want to link.
5. Enter a network location defined in Application Analytics and click **OK**
6. The map link is added to the map. You can reposition the map, if desired, or edit a link by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the

menu.

7. Click the **Save** button to save the map.

NOTE: You can edit a map link created before link locations were supported by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu. This allows you to specify a location for a link without having to delete and re-add the link.

Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per floorplan

A single floorplan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floorplan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

Related Information

- Extreme Management Center Maps Overview
- How to Create and Edit Maps

How to Design Floorplans

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) allow you to design and enhance custom floorplans of your wired and wireless network environment using drawing tools and the style menu.

Designing a Floorplan

Using the drawing and style tools, you can create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

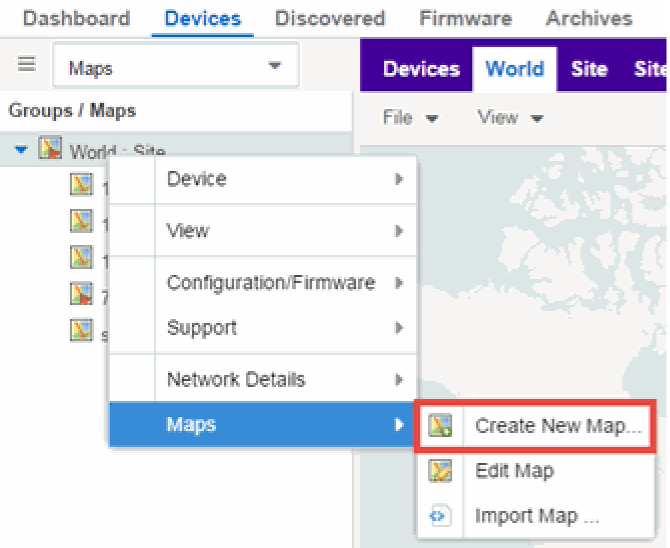
A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image.

(The Map feature supports images in .png, .gif, and .jpg formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thicknesses, and wall colors to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provides greater accuracy in wireless calculations.

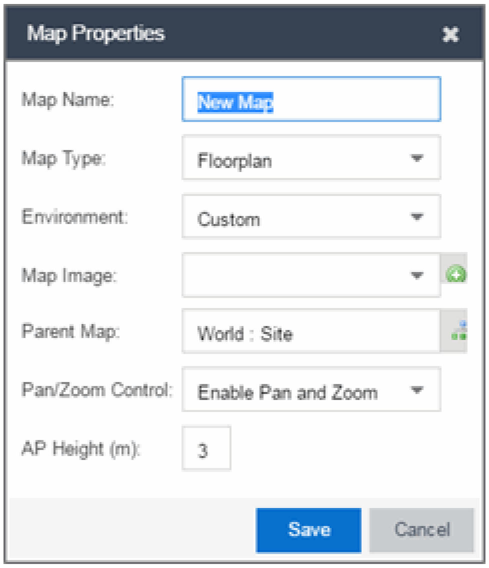
1. Create and configure a new map.
   a. Launch Extreme Management Center and click on the **Network** > **Devices** tab.
   b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

   c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



Map Properties

Map Name: New Map

Map Type: Floorplan

Environment: Custom

Map Image:

Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

AP Height (m): 3

e. Change the **Map Type** drop-down menu to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in the .png, .gif, and .jpg formats. The maximum image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

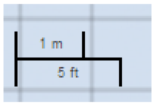
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

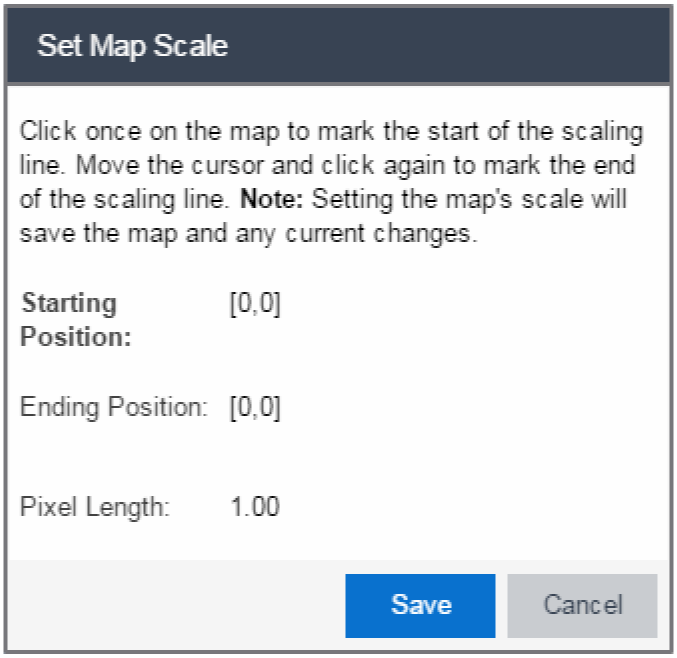
i. Click **Save** to save the map and display the image.

2. **Set the map** scale. It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Click **File** > **Edit** to open the map in edit mode.

   b. Click on the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)





Set Map Scale

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. **Note:** Setting the map's scale will save the map and any current changes.

Starting Position: [0,0]

Ending Position: [0,0]

Pixel Length: 1.00

c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

   i. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.

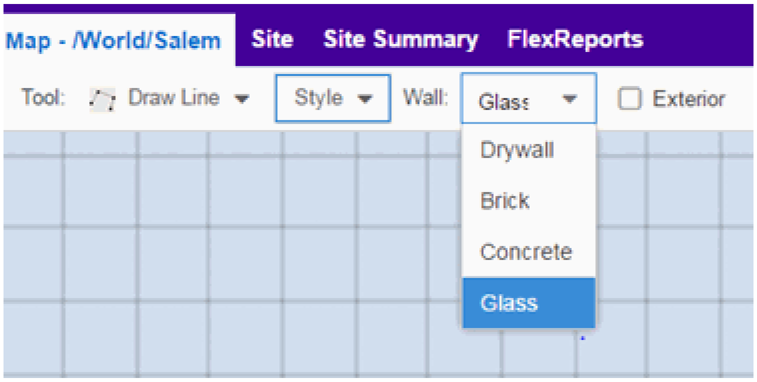
   ii. Enter the line length and units.

d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down menu and select the checkbox to specify that the wall is an exterior wall.



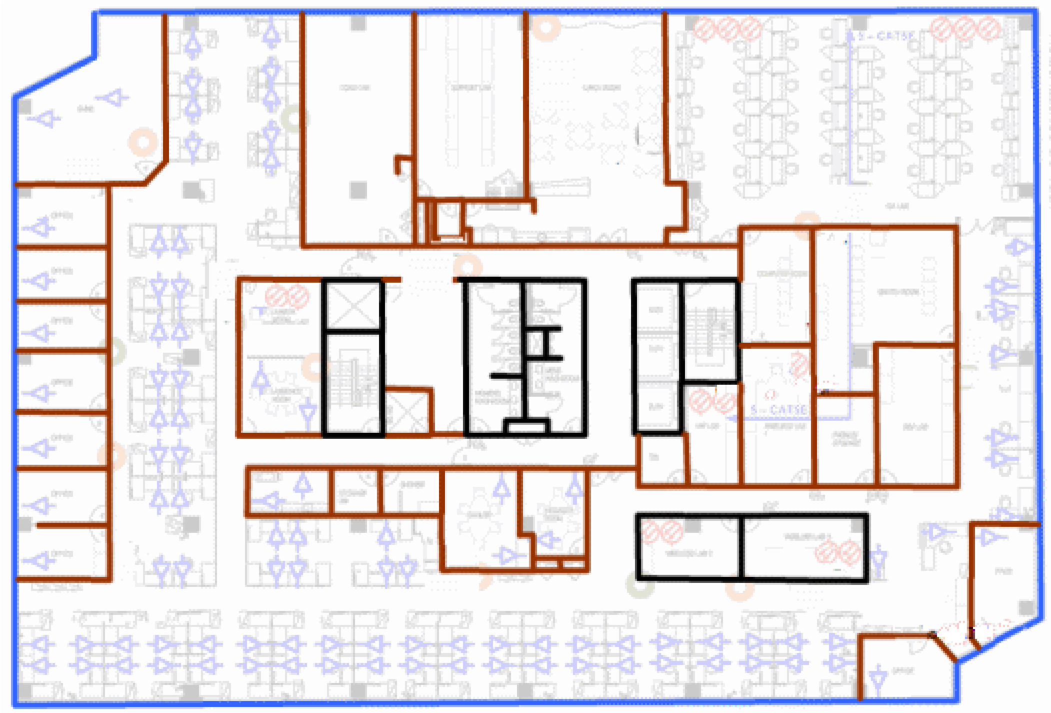
c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

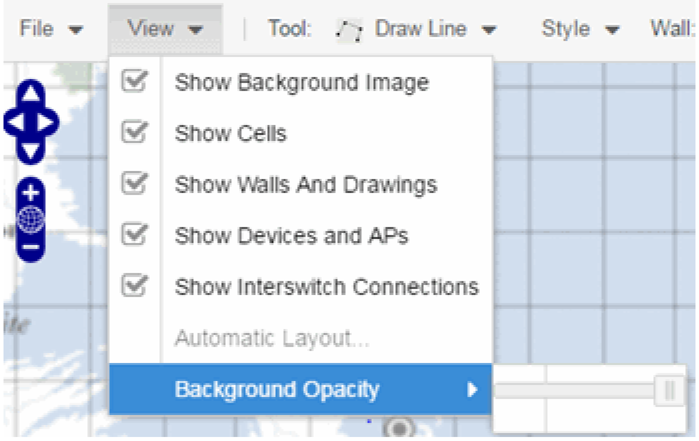
You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, click **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



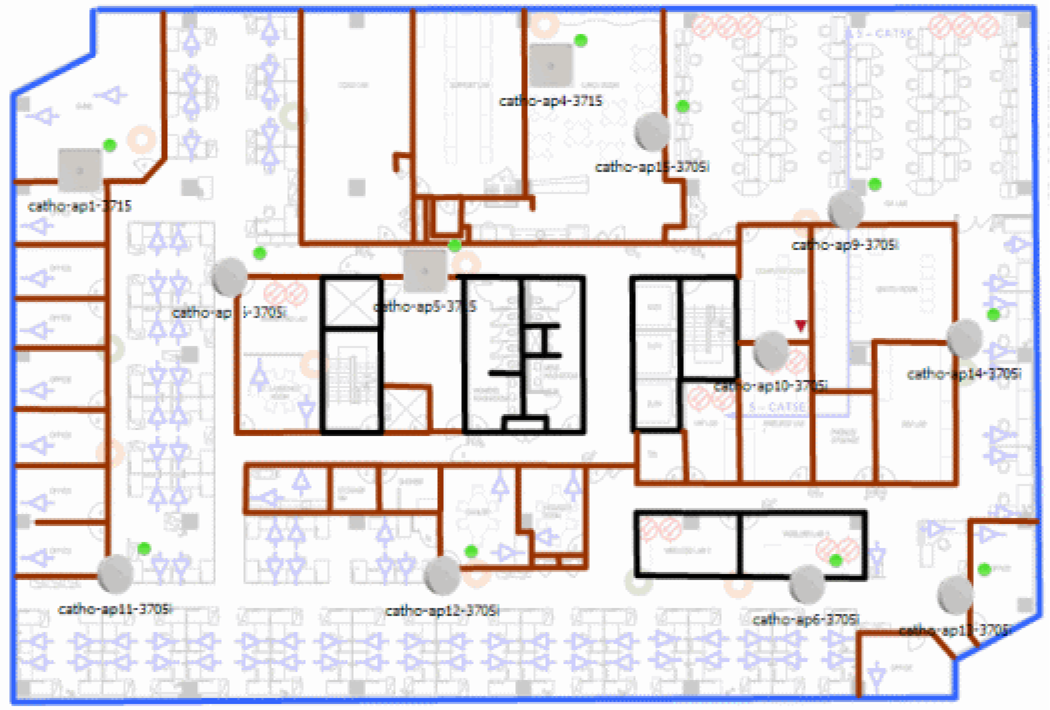
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



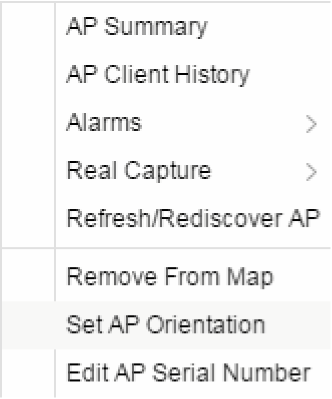
4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You

can use the search field to locate a specific device or AP.

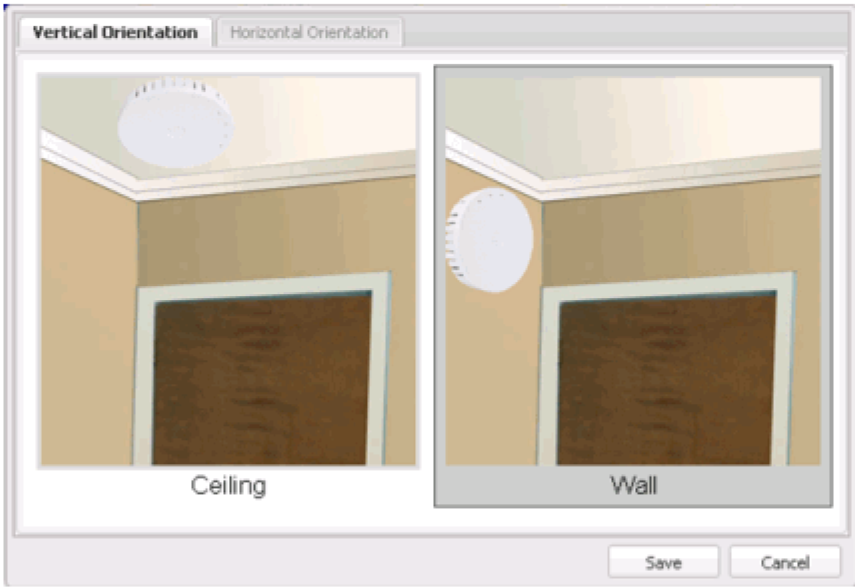
Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.



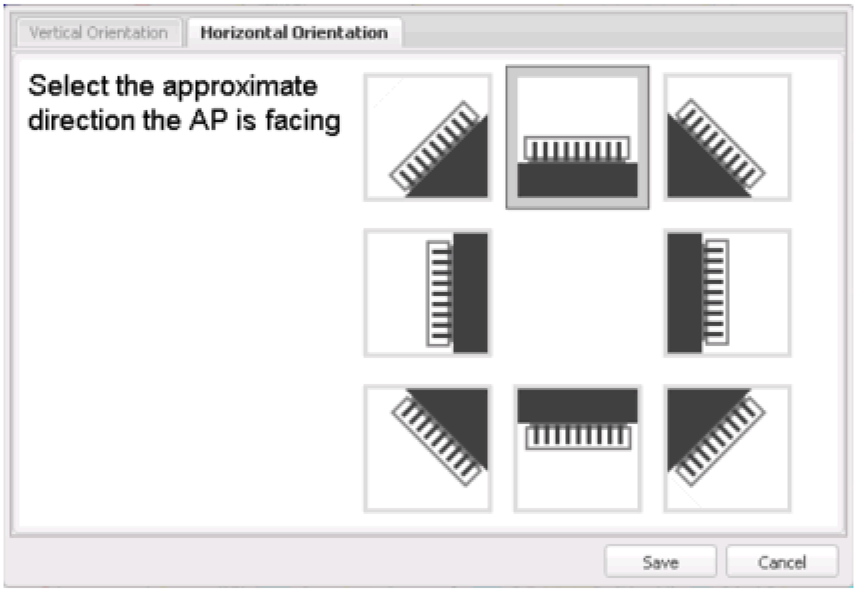
5. Set AP orientation.
   a. Right-click on an AP in the map and select **Set AP Orientation**.



   b. Click on the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.

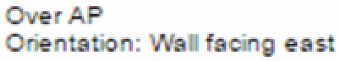


c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



Select the approximate direction the AP is facing

d. Click **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.



Over AP
Orientation: Wall facing east

6. Click **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and wireless coverage information.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down menu to specify whether to:
   - Display markers instead of device images on your map
   - Display cells on the map image to show the map's actual image area
   - Display AP channel information (if available)
   - Display walls and drawings
   - Show application data for map links (if available)
   - Set the map's background opacity
   - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the **Tool** menu.

Drawing Tool	Definition
✋	**Select Items** Click on a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Click anywhere on the map and drag to reposition the map image.
▱	**Draw Area** Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.

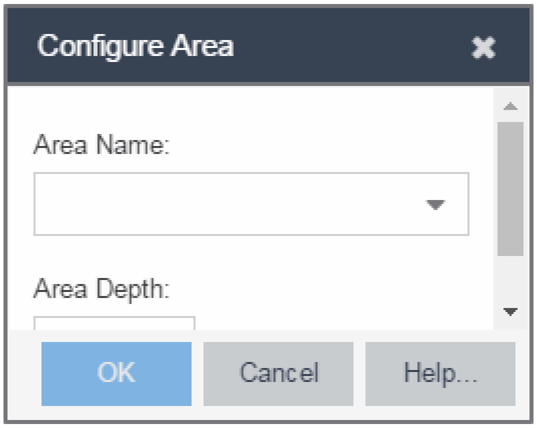
Drawing Tool	Definition
⬠	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the 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.
✎	**Add Text** Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click to add the text to your map. Use the **Style** menu to change the text appearance.
△	**Draw Triangle** Position the cursor where you want the triangle. Click and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	Draw Line Position your cursor where you want to start drawing the line. Click once and draw the line. Click to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
↻	**Rotate Shape** Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
	Set Scale Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

NOTE: The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.

Style Option	Description
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from Extreme Management Center Devices and Wireless

Using the Extreme Management Center Maps feature, you can quickly add devices and wireless access points (APs) to your maps directly from the Devices list or from the navigation tree on the Extreme Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

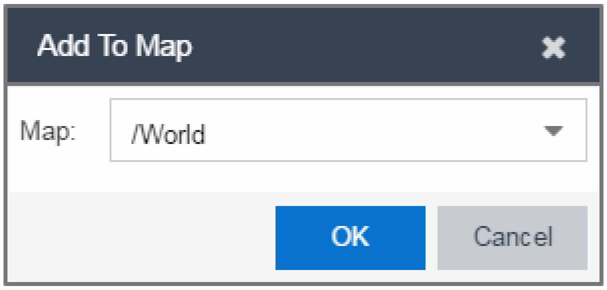
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the **Network** tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down menu in the left-panel.

2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Add to Map**.
3. In the Add to Map window, use the drop-down menu to select the desired map. Click **OK** to add the devices or APs to the map.


Add To Map

Map: /World

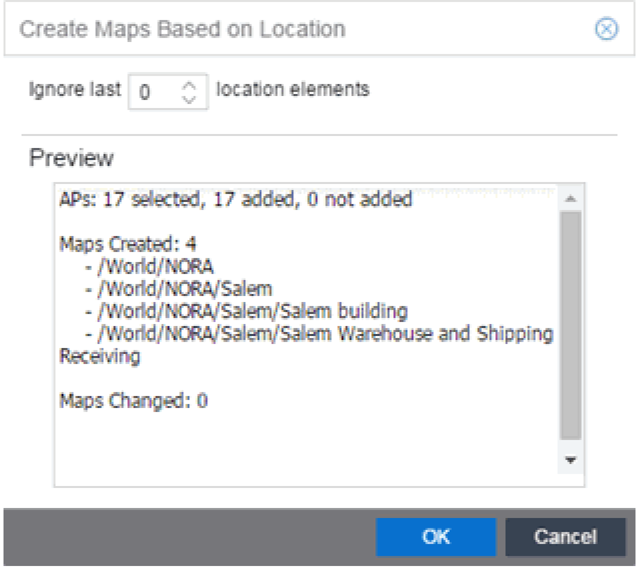
4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be created to the Third Floor level, and then you manually position the devices in the correct location on the map.

1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, click on the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 9 APs to a map. This creates eight new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.

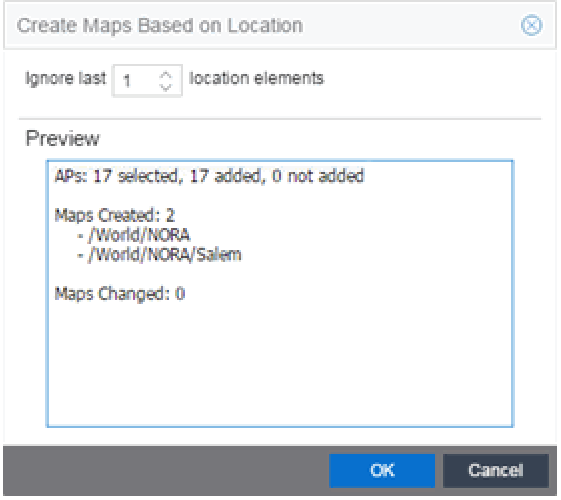


APs: 17 selected, 17 added, 0 not added

Maps Created: 4
- /World/NORA
- /World/NORA/Salem
- /World/NORA/Salem/Salem building
- /World/NORA/Salem/Salem Warehouse and Shipping Receiving

Maps Changed: 0

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.



APs: 17 selected, 17 added, 0 not added

Maps Created: 2
- /World/NORA
- /World/NORA/Salem

Maps Changed: 0

3. Click **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps.
5. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
6. Click the **Save** button to save the devices/APs to the map.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Display Map Application Data

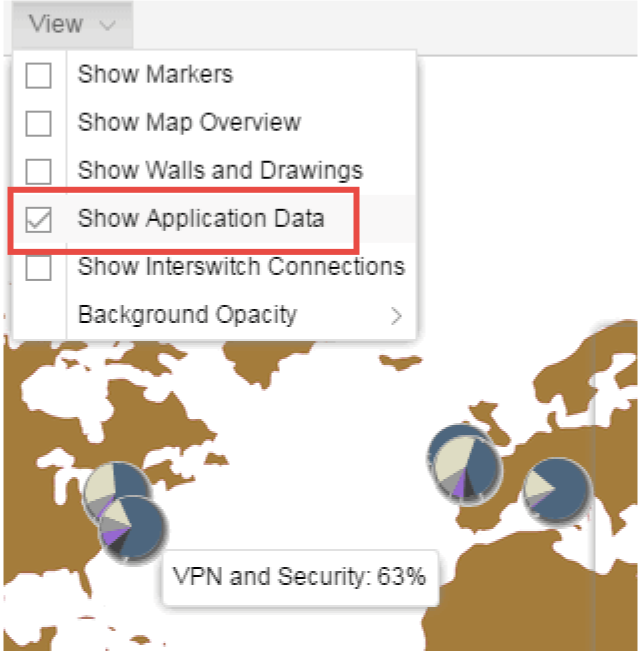
The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) allows you to display application data in maps by creating map links tied to ExtremeAnalytics network locations. Application data for the location tied to the link displays in the map.

Show Application Data

When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the Location field specified for the link and corresponds to a network location defined in the ExtremeAnalyticsfeature. For more information on network locations, see the section on Network Locations in the ExtremeAnalytics user guide.

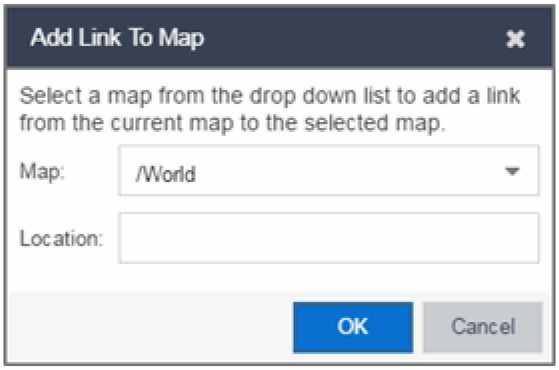
The pie chart displays the top five application groups (by bytes transferred) for the location specified for the map link.

Rest the cursor over the pie chart to view a tooltip. If there is no application data, nothing displays.



Adding a Map Link with Location

1. In the Maps navigation tree, right-click on the map you want to link from and select **Maps** > **Edit Map** or click **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Click **File** > **Add** > **Map Link**.
3. The Add Link to Map window opens.



Add Link To Map

Select a map from the drop down list to add a link from the current map to the selected map.

Map: /World

Location:

4. From the drop-down list, select the map to which you want to link.
5. Enter a network location defined in ExtremeAnalytics and click **OK.**
6. The map link is added to the map. You can reposition the map, if desired, or edit a link by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the

menu.

7. Click the **Save** button to save the map.

NOTE: You can edit a map link created before link locations were supported by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu. This allows you to specify a location for a link without having to delete and re-add the link.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

How to Use Maps to Locate Wireless Clients

The **Network** > **Devices** tab in the Extreme Management Centercontains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network.

The advanced map features (available with the NMS-ADV license) allow you to design and enhance custom floorplans of your wired and wireless network environment. The wireless location feature provides the ability, using historic triangulated location results, to view time-lapse location coverage for a client. This allows you to understand a wireless client's movement through the network and provides for better network troubleshooting.

This topic also provides information about limits for wireless client location and wireless coverage maps.

Wireless Client Location

The wireless location feature requires you enable the location engine on the wireless controller. Once you add APs to your custom floor plan and save the map, a copy of the floorplan is sent to each controller.

The location engine incorporates information defined in the floorplan data and signal information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to determine a client's triangulated location.

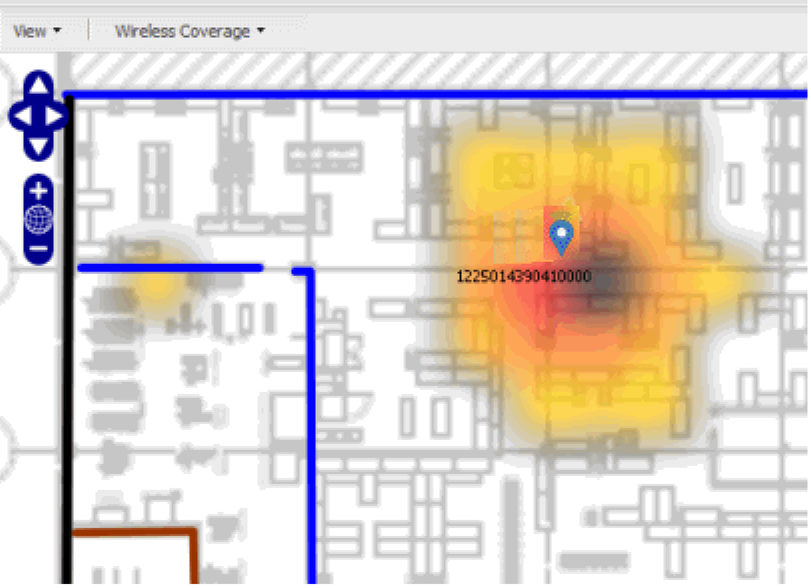
To search for a wireless client:

1. Launch Extreme Management Center.
2. In the **SearchNetwork** box, click **Advanced** .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information in the open **Search** box.
4. Press **Enter**. (The client must be connected to an AP added to a map.)

   The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence.

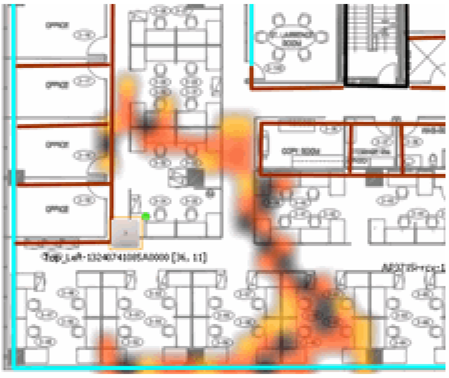
5. On the View tab, use the **Min. Location Confidence** slider to filter out lower confidence colors:
   a. Drag the slider to eliminate colors below the selected confidence level
   b. Drag the slider all the way to the right to display only black.
6. Mouse over the client icon to see a tooltip with client information.

NOTE: The tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the **Wireless** > **Clients** tab and the confidence colors are not displayed.

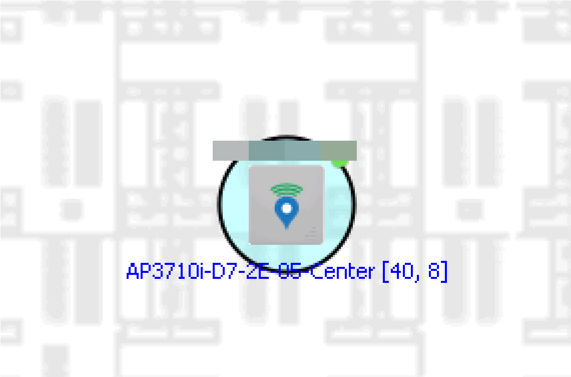


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.



If there is insufficient data to provide triangulated results, the map displays the AP in the center, with a circle showing the possible area where the client may be located, based on the client's RSS (Received Signal Strength).

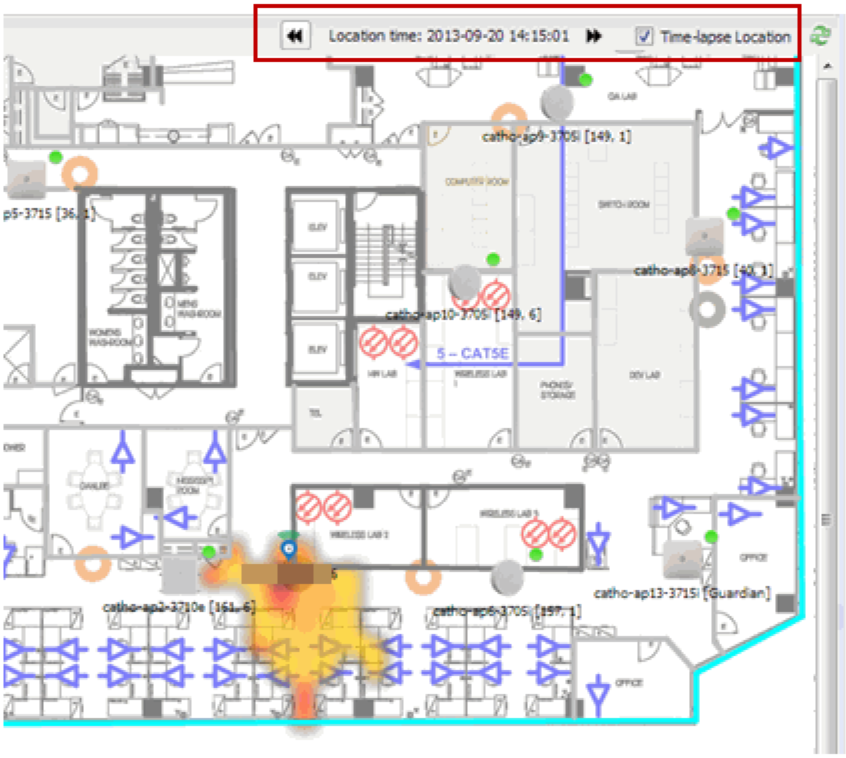


Time-Lapse Location

To enable time-lapse location:

1. Click the Time-Lapse Location checkbox in the upper right corner of the a triangulated location search result window.
2. Locate the set of controls that appears to the left of the checkbox that indicate the date of the displayed result.
3. If there are historic events available, the Rewind and Fast-Forward arrows are enabled:
    a. Click the left arrow to rewind.

b. Click the right arrow to fast-forward.



Location time: 2013-09-20 14:15:01

☑ Time-lapse Location

NOTES: Note that for a historic location, the client icon displays a small clock inside it.
The Rewind and Fast-Forward arrows are disabled if there is no more history in that direction.
After viewing historic locations, if you fast forward to the current location and it changed, the location updates.

Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients that the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per Floor Plan

A single floor plan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floor plan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

How to View Wireless Coverage

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) include wireless coverage maps to identify coverage trouble spots for your wireless network.

Wireless Coverage

After you finish your custom floor plan and save the map, the map is ready to display wireless coverage information.

1. Select **View** > **Wireless Coverage** > **Show Coverage** to show wireless coverage of the APs on the map and to enable the wireless coverage options.
2. Use the **View** > **Wireless Coverage** menu available at the top of the map to select from the following coverage display options.

- Mode — Select from the different options for coverage display:
  - Signal Strength— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
  - Channel Coverage — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This mode provides a graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.
  - Data Rate — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and Access Points options. Use this mode to ensure proper wireless performance throughout the network.

NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

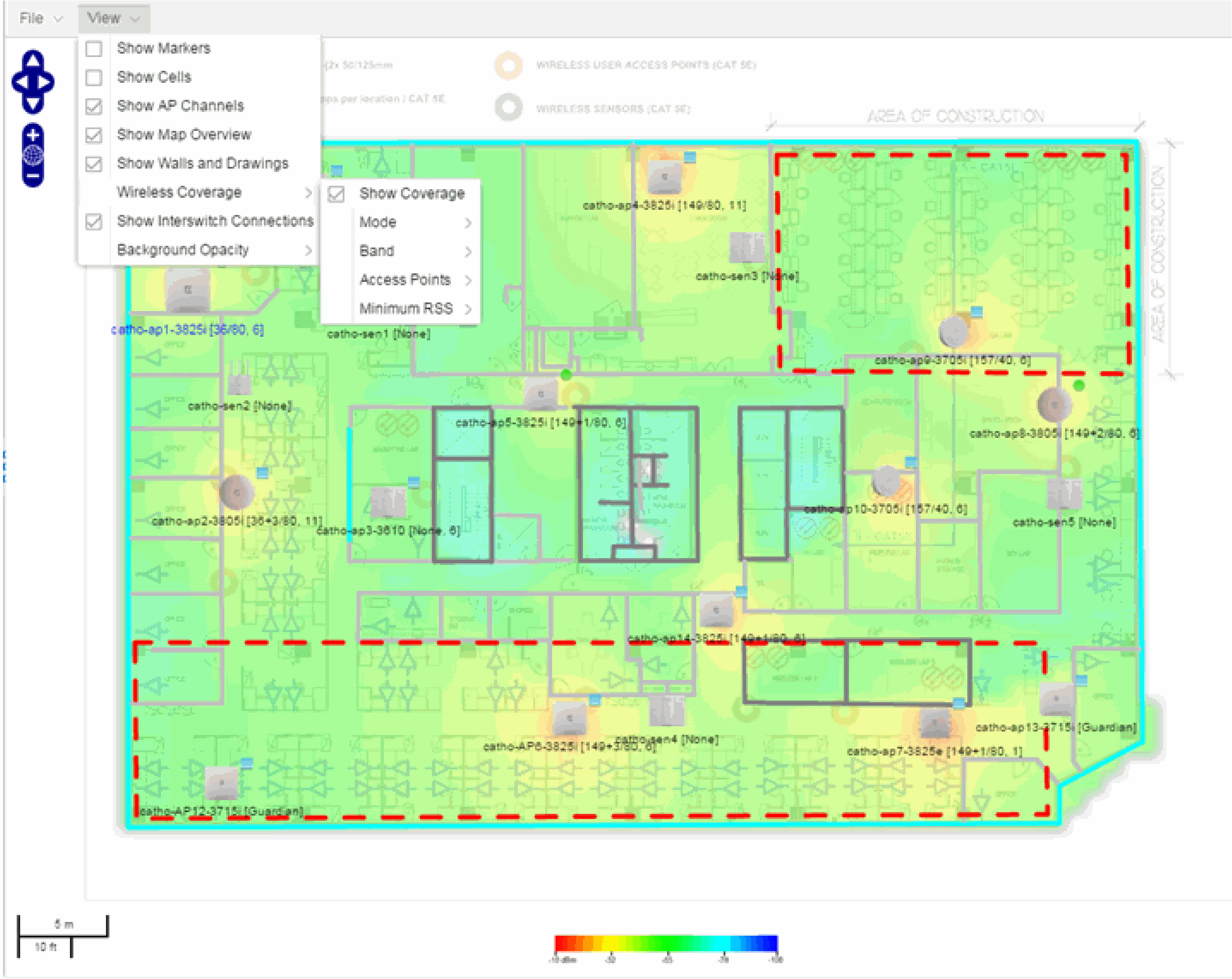
  - Location Readiness — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
    - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
    - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
    - Orange — Poor readiness. There are less than three APs with visibility of the cell.
    - Red — No triangulation. Only Cell of Origin location results are available in this area.
- Select Channel — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
  - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission

of other stations or APs. This is an indicator of the congestion and interference on the channel.

  - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.

- Min. Physical Rate — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- Band — Select the desired band (radio frequency).
- Access Points — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- Minimum RSS — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

Once these options are set, the map displays the selected coverage information. The following map shows signal strength coverage.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage
☑ Show Interswitch Connections
Background Opacity
☑ Show Coverage
Mode
Band
Access Points
Minimum RSS
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
AREA OF CONSTRUCTION
AREA OF CONSTRUCTION
catho-ap1-3825i [36/80, 6]
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-sen1 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-3805i [149+2/80, 6]
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-sen5 [None]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap13-3715i [Guardian]
catho-ap7-3825e [149+1/80, 1]
catho-AP12-3715i [Guardian]
5 m
10 ft
-10 dBm
-32
-55
-78
-100

Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per Floor Plan

A single floor plan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floor plan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

How to Export Maps

The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

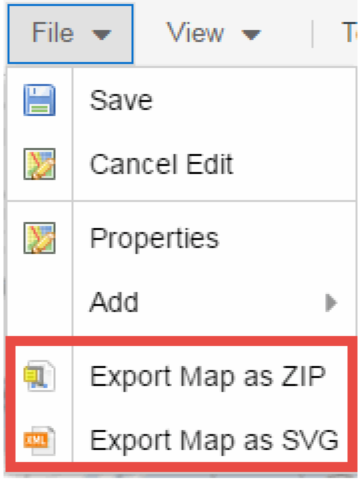
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) include the map export function, which gives you the ability to export floor plan maps as a ZIP or SVG file.

Exporting Maps

1. Launch Extreme Management Center and click on the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.

3. The map opens in Edit mode. Click **File** > **Export Map as ZIP** or **Export Map as SVG**.



- If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browser's default download location.

  NOTE: The Export Map as ZIP option is only available for floorplan map types.

- If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Design Floorplans

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) allow you to design and enhance custom floorplans of your wired and wireless network environment using drawing tools and the style menu.

Designing a Floorplan

Using the drawing and style tools, you can create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

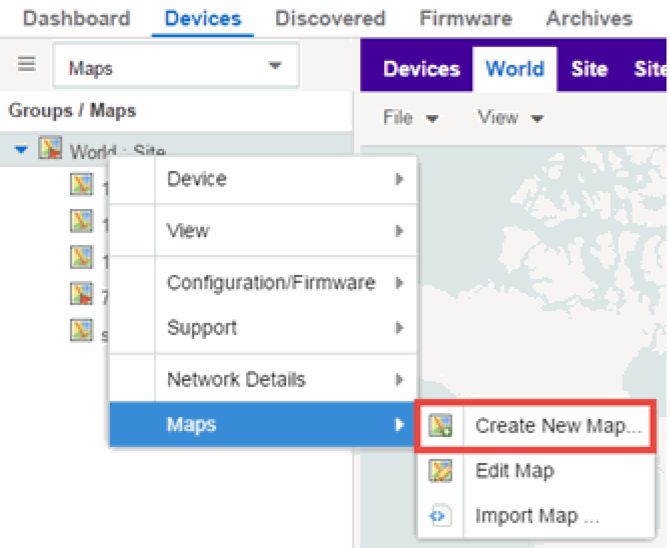
A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image. (The Map feature supports images in .png, .gif, and .jpg formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thicknesses, and wall colors to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and

APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provides greater accuracy in wireless calculations.

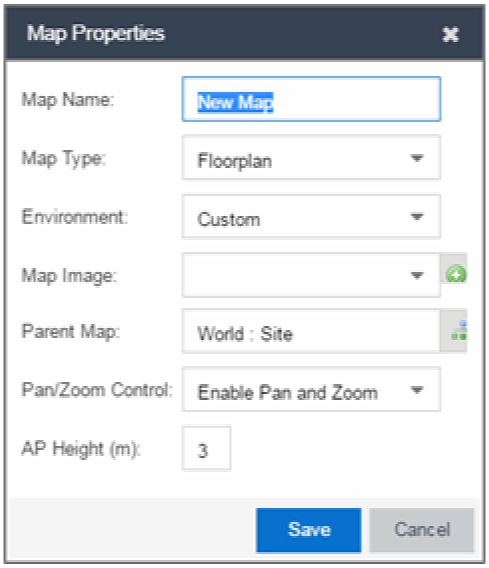
1. Create and configure a new map.
   a. Launch Extreme Management Center and click on the **Network** > **Devices** tab.
   b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



   The Create New Map window opens.

   c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



Map Properties

Map Name: New Map

Map Type: Floorplan

Environment: Custom

Map Image:

Parent Map: World : Site

Pan/Zoom Control: Enable Pan and Zoom

AP Height (m): 3

e. Change the **Map Type** drop-down menu to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in the .png, .gif, and .jpg formats. The maximum image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

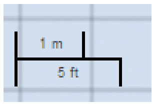
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

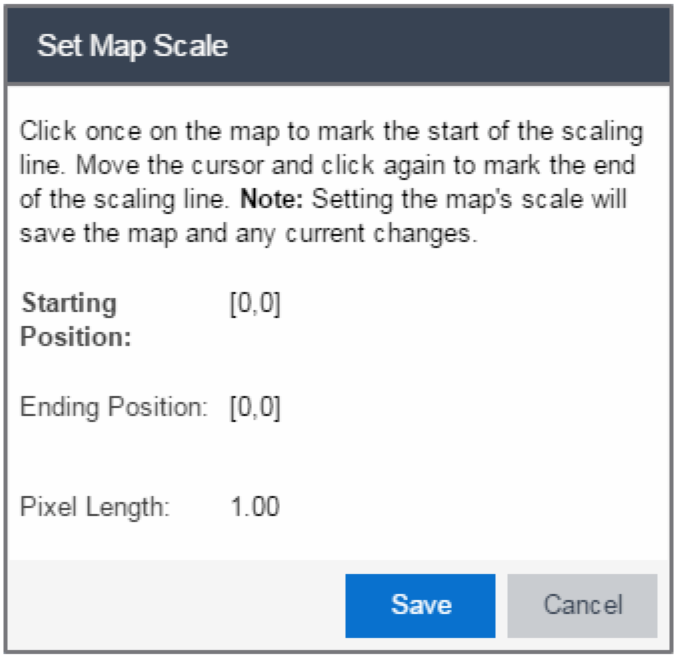
i. Click **Save** to save the map and display the image.

2. **Set the map** scale. It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Click **File** > **Edit** to open the map in edit mode.

   b. Click on the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)





Set Map Scale

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. **Note:** Setting the map's scale will save the map and any current changes.

Starting Position:	[0,0]
Ending Position:	[0,0]
Pixel Length:	1.00

c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

   i. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.

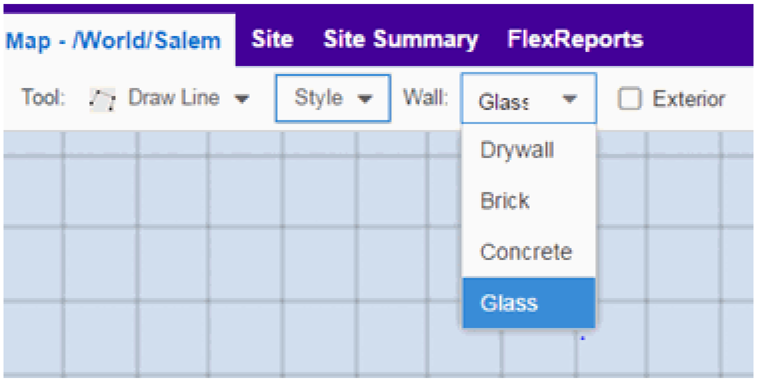
   ii. Enter the line length and units.

d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down menu and select the checkbox to specify that the wall is an exterior wall.



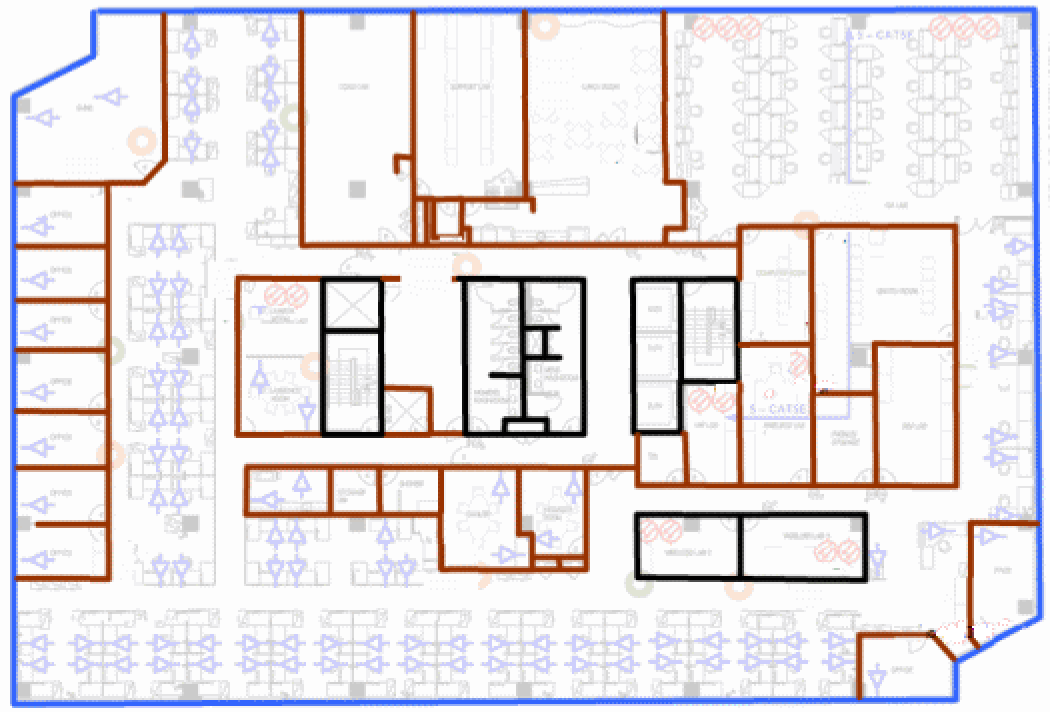
c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

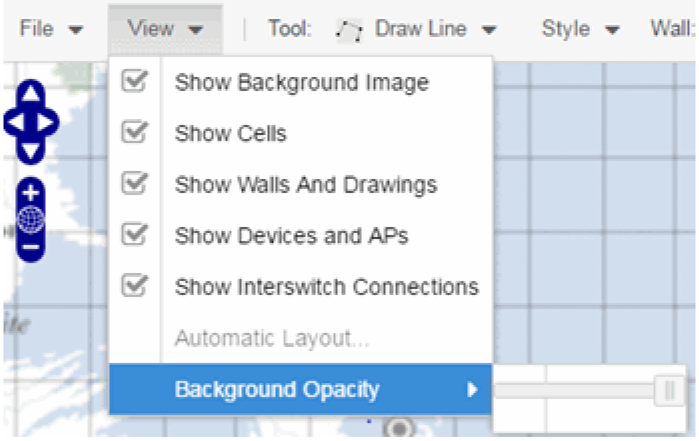
You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, click **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



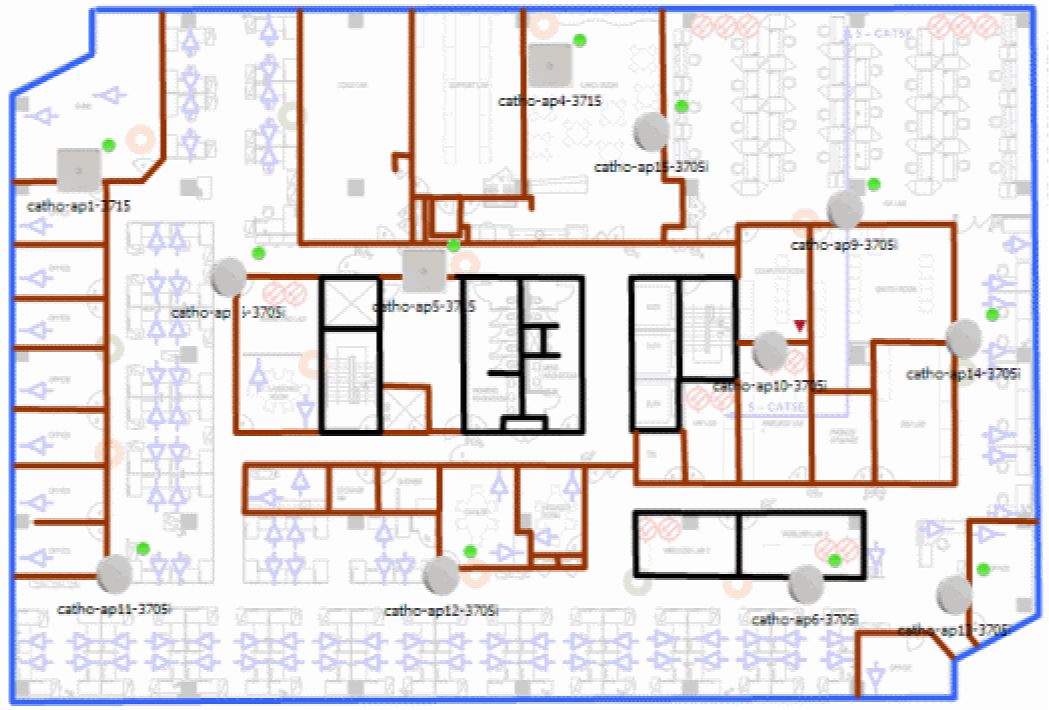
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You

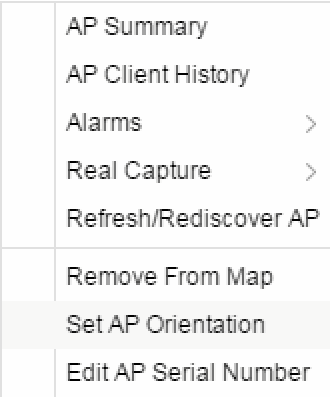
can use the search field to locate a specific device or AP.

Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.

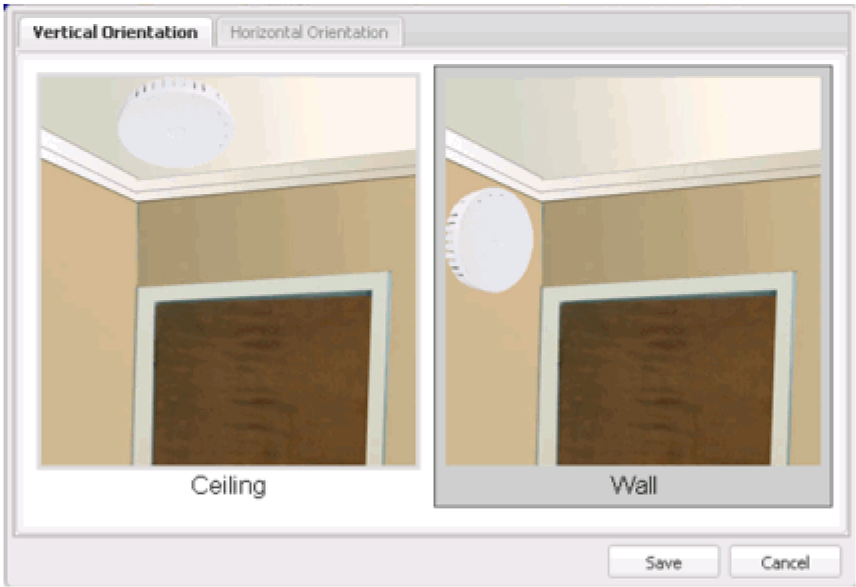


5. Set AP orientation.

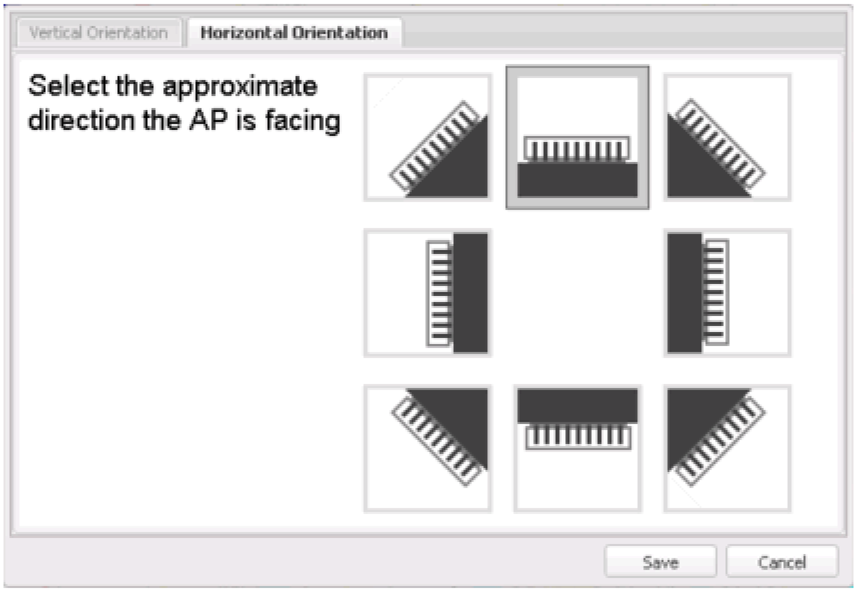
   a. Right-click on an AP in the map and select **Set AP Orientation**.



   b. Click on the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.



c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



d. Click **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.

Over AP
Orientation: Wall facing east

6. Click **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and wireless coverage information.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down menu to specify whether to:
   - Display markers instead of device images on your map
   - Display cells on the map image to show the map's actual image area
   - Display AP channel information (if available)
   - Display walls and drawings
   - Show application data for map links (if available)
   - Set the map's background opacity
   - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the **Tool** menu.

Drawing Tool	Definition
✋	**Select Items** Click on a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Click anywhere on the map and drag to reposition the map image.
▱	Draw Area Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.

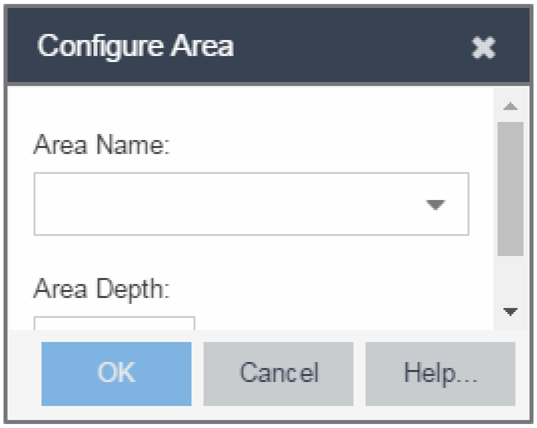
Drawing Tool	Definition
⬠	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw 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.
✎	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click to add the text to your map. Use the **Style** menu to change the text appearance.
△	Draw Triangle Position the cursor where you want the triangle. Click and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
⌒	Draw Line Position your cursor where you want to start drawing the line. Click once and draw the line. Click to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
↻	Rotate Shape Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
⬚	Set Scale Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

NOTE: The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.

Style Option	Description
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Export Maps

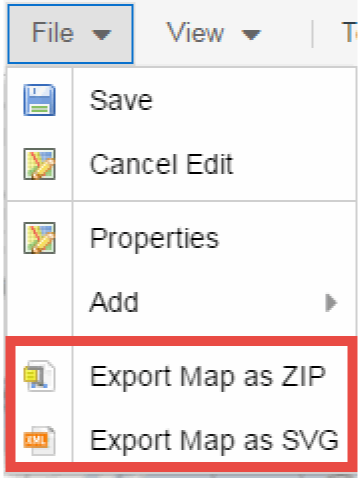
The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) include the map export function, which gives you the ability to export floor plan maps as a ZIP or SVG file.

Exporting Maps

1. Launch Extreme Management Center and click on the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.
3. The map opens in Edit mode. Click **File** > **Export Map as ZIP** or **Export Map as SVG**.



- If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browser's default download location.

  NOTE: The Export Map as ZIP option is only available for floorplan map types.

- If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **EAPS tab** allows you to access information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

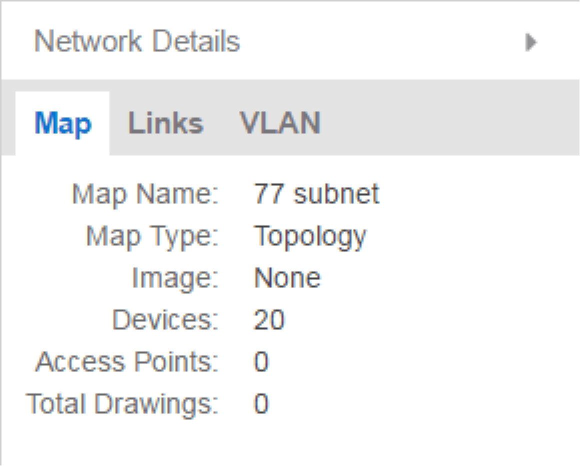
1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

1. Right-click the map or map tree in the left-panel.
2. Click **Network Details** from the drop-down menu. Several additional tabs are available, depending on the devices included in the map:
    a. EAPS Summary tab — Lists information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.
    b. Link Summary tab — Displays information about the network connections between devices
    c. VLAN Summary tab — Lists any virtual local area networks within the map
    d. MLAG Summary tab — Lists devices configured in a multi-switch link aggregation group
    e. VPLS Summary tab — Displays information about site connectivity within a private VLAN

NOTE: For an alternate way to access the additional tabs:

1. Click **Network > Devices**
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **Network Details** panel at the far right. The panel also includes a Map tab that displays basic information about the map, including the name of the map, the map type, and the background image, as well as the number of devices, APs, and drawings on the map.



Map Name: 77 subnet
Map Type: Topology
Image: None
Devices: 20
Access Points: 0
Total Drawings: 0

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the EAPS tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **EAPS tab** allows you to access information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

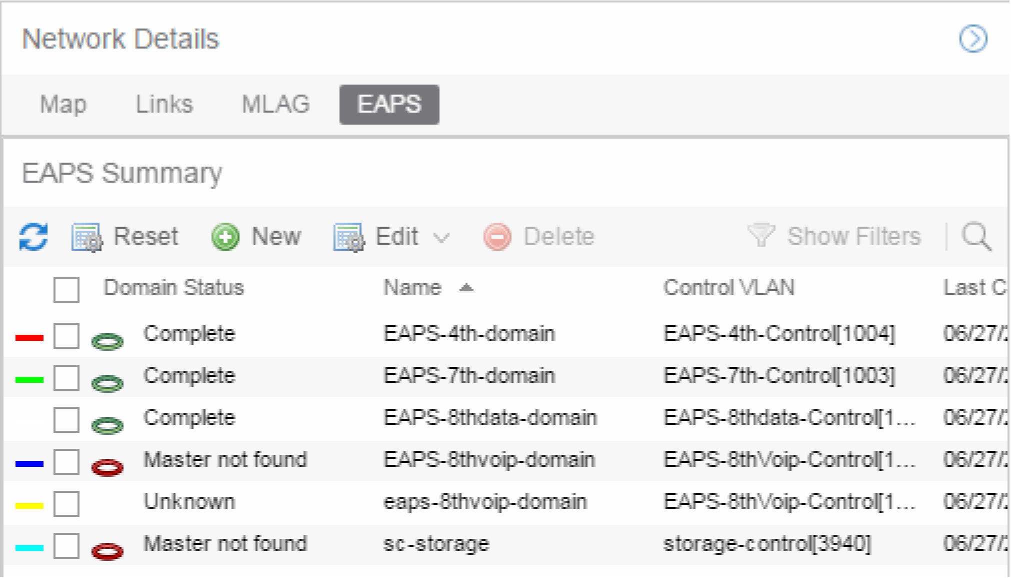
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down menu.
3. Select **EAPS Summary.**

NOTE: For an alternate way to access the EAPS Summary tab:

1. Click **Network** > **Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **EAPS** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

EAPS Summary Tab

The **EAPS Summary tab** displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



Network Details

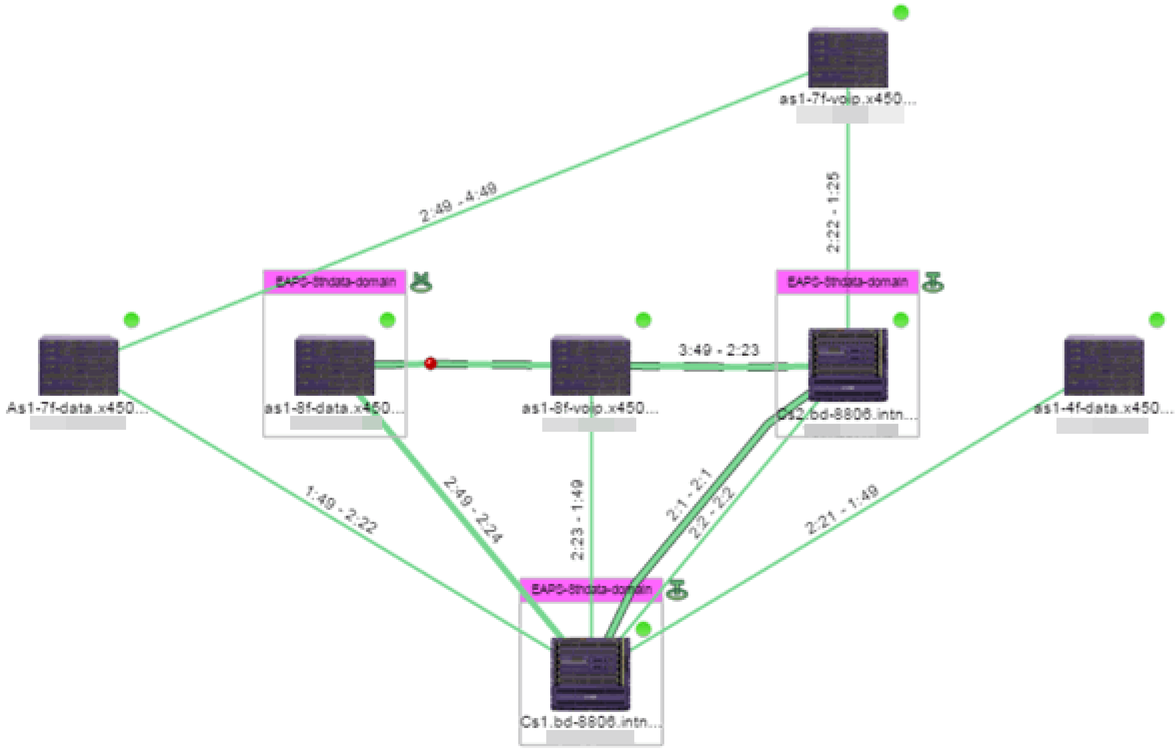
Map | Links | MLAG | **EAPS**

EAPS Summary

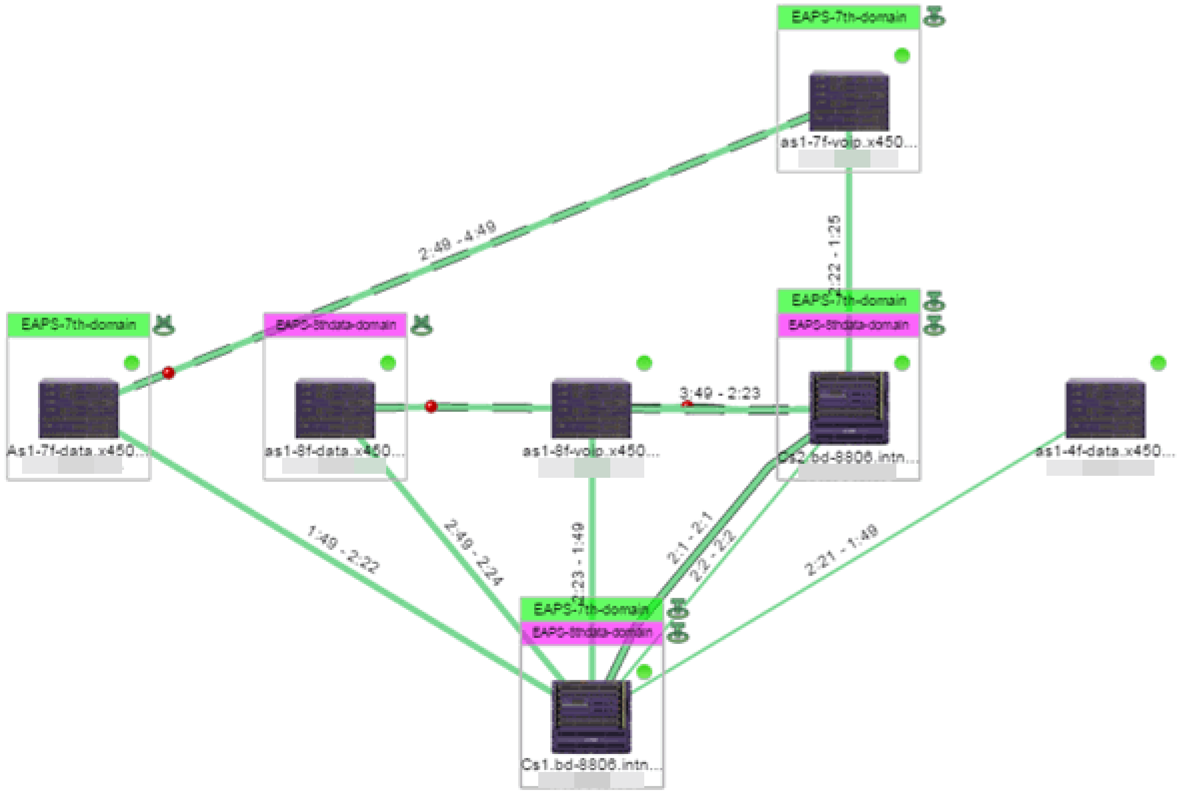
Reset | New | Edit | Delete | Show Filters

	□		Domain Status	Name ▲	Control VLAN	Last C
🟥	□	○	Complete	EAPS-4th-domain	EAPS-4th-Control[1004]	06/27/
🟩	□	○	Complete	EAPS-7th-domain	EAPS-7th-Control[1003]	06/27/
	□	○	Complete	EAPS-8thdata-domain	EAPS-8thdata-Control[1...	06/27/
🟦	□	○	Master not found	EAPS-8thvoip-domain	EAPS-8thVoip-Control[1...	06/27/
🟨	□		Unknown	eaps-8thvoip-domain	EAPS-8thVoip-Control[1...	06/27/
🟦	□	○	Master not found	sc-storage	storage-control[3940]	06/27/

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.

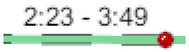


An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon, or if the node is a transit node, indicated by a "T" icon.

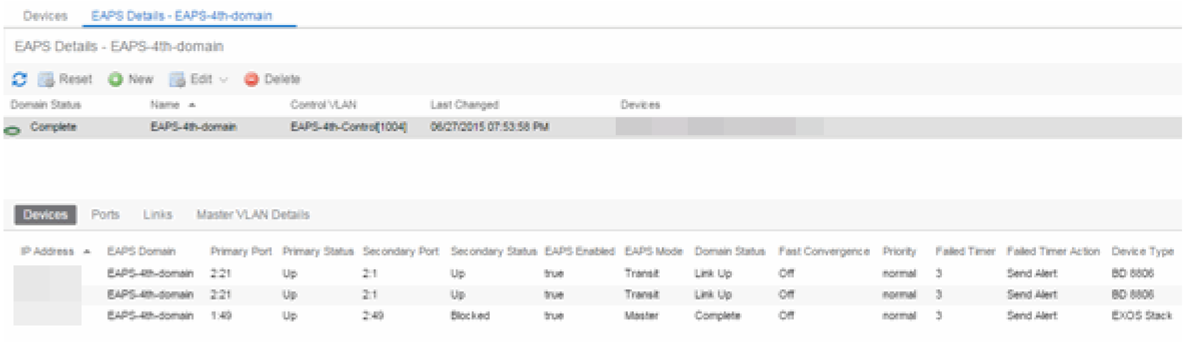
The color of the ring icon indicates the status of the domain:

- 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.



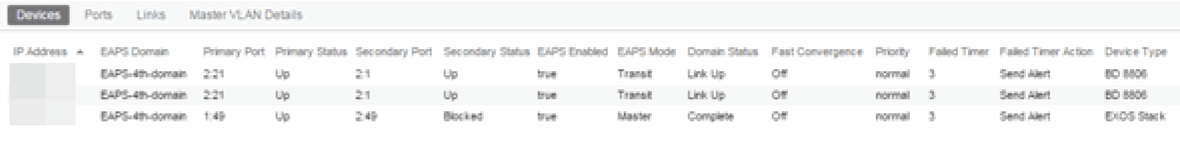
EAPS Details - EAPS-4th-domain

Domain Status	Name	Control VLAN	Last Changed	Devices
Complete	EAPS-4th-domain	EAPS-4th-Control[1004]	06/27/2015 07:53:58 PM	[redacted]

IP Address	EAPS Domain	Primary Port	Primary Status	Secondary Port	Secondary Status	EAPS Enabled	EAPS Mode	Domain Status	Fast Convergence	Priority	Failed Timer	Failed Timer Action	Device Type
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	1:49	Up	2:49	Blocked	true	Master	Complete	Off	normal	3	Send Alert	EXOS Stack

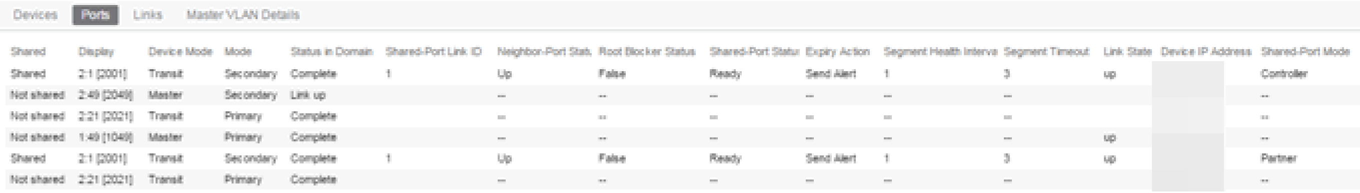
The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

- **Devices** — Displays information about the devices using the EAPS domain.



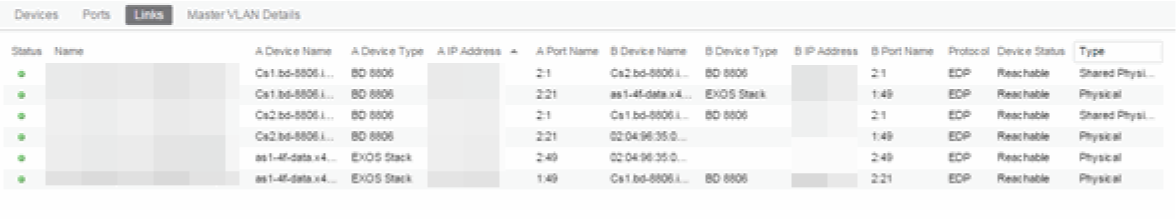
IP Address	EAPS Domain	Primary Port	Primary Status	Secondary Port	Secondary Status	EAPS Enabled	EAPS Mode	Domain Status	Fast Convergence	Priority	Failed Timer	Failed Timer Action	Device Type
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	2:21	Up	2:1	Up	true	Transit	Link Up	Off	normal	3	Send Alert	BD 8806
[redacted]	EAPS-4th-domain	1:49	Up	2:49	Blocked	true	Master	Complete	Off	normal	3	Send Alert	EXOS Stack

- **Ports** — Displays information about the shared ports associated with the EAPS domain.



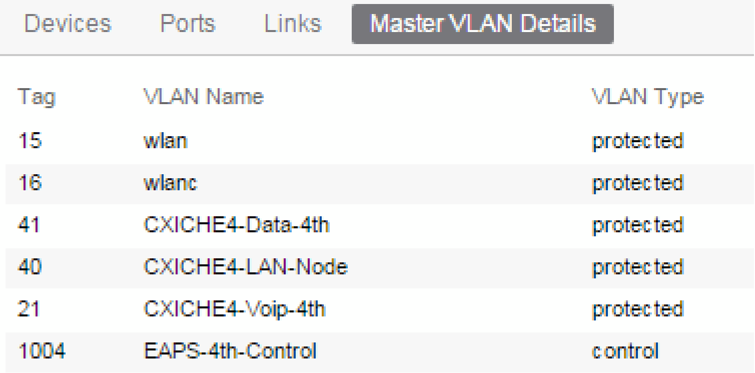
Shared	Display	Device Mode	Mode	Status in Domain	Shared-Port Link ID	Neighbor-Port Stat.	Root Blocker Status	Shared-Port Statu	Expiry Action	Segment Health Interva	Segment Timeout	Link State	Device IP Address	Shared-Port Mode
Shared	2:1 [2001]	Transit	Secondary	Complete	1	Up	False	Ready	Send Alert	1	3	up	[redacted]	Controller
Not shared	2:49 [2049]	Master	Secondary	Link up		--	--	--	--	--	--		[redacted]	--
Not shared	2:21 [2021]	Transit	Primary	Complete		--	--	--	--	--	--		[redacted]	--
Not shared	1:49 [1049]	Master	Primary	Complete		--	--	--	--	--	--	up	[redacted]	--
Shared	2:1 [2001]	Transit	Secondary	Complete	1	Up	False	Ready	Send Alert	1	3	up	[redacted]	Partner
Not shared	2:21 [2021]	Transit	Primary	Complete		--	--	--	--	--	--		[redacted]	--

- **Links** — Displays links between devices using the EAPS domain.



Status	Name	A Device Name	A Device Type	A IP Address	A Port Name	B Device Name	B Device Type	B IP Address	B Port Name	Protocol	Device Status	Type
●	[redacted]	Cs1.bd-8806.i...	BD 8806	[redacted]	2:1	Cs2.bd-8806.i...	BD 8806	[redacted]	2:1	EDP	Reachable	Shared Physi...
●	[redacted]	Cs1.bd-8806.i...	BD 8806	[redacted]	2:21	as1-4f-data.x4...	EXOS Stack	[redacted]	1:49	EDP	Reachable	Physical
●	[redacted]	Cs2.bd-8806.i...	BD 8806	[redacted]	2:1	Cs1.bd-8806.i...	BD 8806	[redacted]	2:1	EDP	Reachable	Shared Physi...
●	[redacted]	Cs2.bd-8806.i...	BD 8806	[redacted]	2:21	02:04:96:35:0...		[redacted]	1:49	EDP	Reachable	Physical
●	[redacted]	as1-4f-data.x4...	EXOS Stack	[redacted]	2:49	02:04:96:35:0...			2:49	EDP	Reachable	Physical
●	[redacted]	as1-4f-data.x4...	EXOS Stack	[redacted]	1:49	Cs1.bd-8806.i...	BD 8806	[redacted]	2:21	EDP	Reachable	Physical

- **Master VLAN Details** — Displays details about the master VLAN associated with the EAPS domain.



Tag	VLAN Name	VLAN Type
15	wlan	protected
16	wlanc	protected
41	CXICHE4-Data-4th	protected
40	CXICHE4-LAN-Node	protected
21	CXICHE4-Voip-4th	protected
1004	EAPS-4th-Control	control

Clicking the **New EAPS Domain** button opens the New EAPS Domain wizard, which allows you to create a create a new EAPS Domain.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the Link Tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **Link Summary tab** displays information about the network connections between devices.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

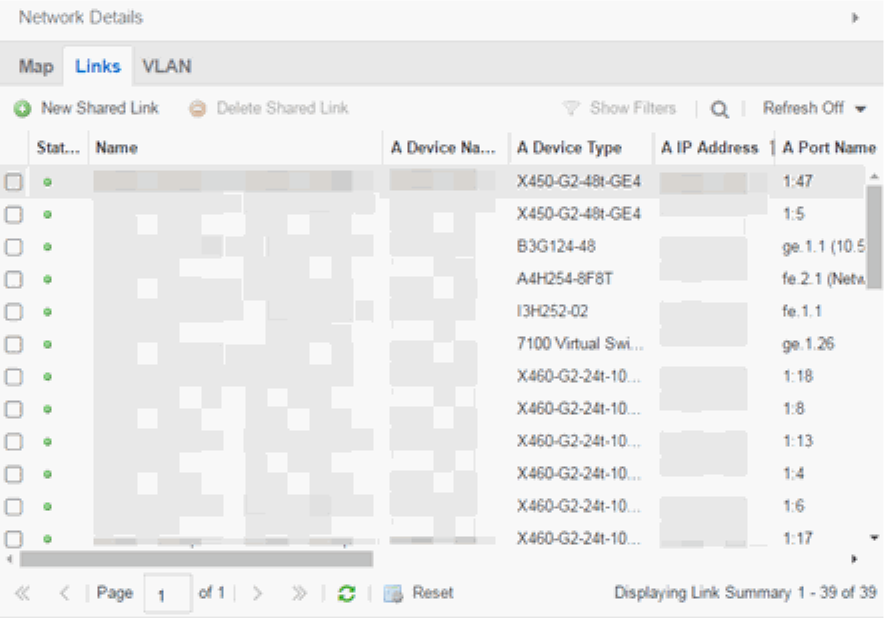
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down menu.
3. Select **Link Summary**.

NOTE: For an alternate way to access the Link Summary tab:

1. Click **Network > Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **Links** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

Link Summary tab

The **Link Summary** tab displays the Link Summary table for maps with one or more network connections, which contains detailed information about the network connections between devices. Selecting one of the links in the table highlights the link in the map.



	Stat...	Name	A Device Na...	A Device Type	A IP Address	A Port Name
☐	●	[redacted]	[redacted]	X450-G2-48t-GE4	[redacted]	1:47
☐	●	[redacted]	[redacted]	X450-G2-48t-GE4	[redacted]	1:5
☐	●	[redacted]	[redacted]	B3G124-48	[redacted]	ge.1.1 (10.5
☐	●	[redacted]	[redacted]	A4H254-8F8T	[redacted]	fe.2.1 (Netw
☐	●	[redacted]	[redacted]	I3H252-02	[redacted]	fe.1.1
☐	●	[redacted]	[redacted]	7100 Virtual Swi...	[redacted]	ge.1.26
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:18
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:8
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:13
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:4
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:6
☐	●	[redacted]	[redacted]	X460-G2-24t-10...	[redacted]	1:17

Displaying Link Summary 1 - 39 of 39

The top of the **Link Summary** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the VLAN tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **VLAN tab** Lists any virtual local area networks within the map.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

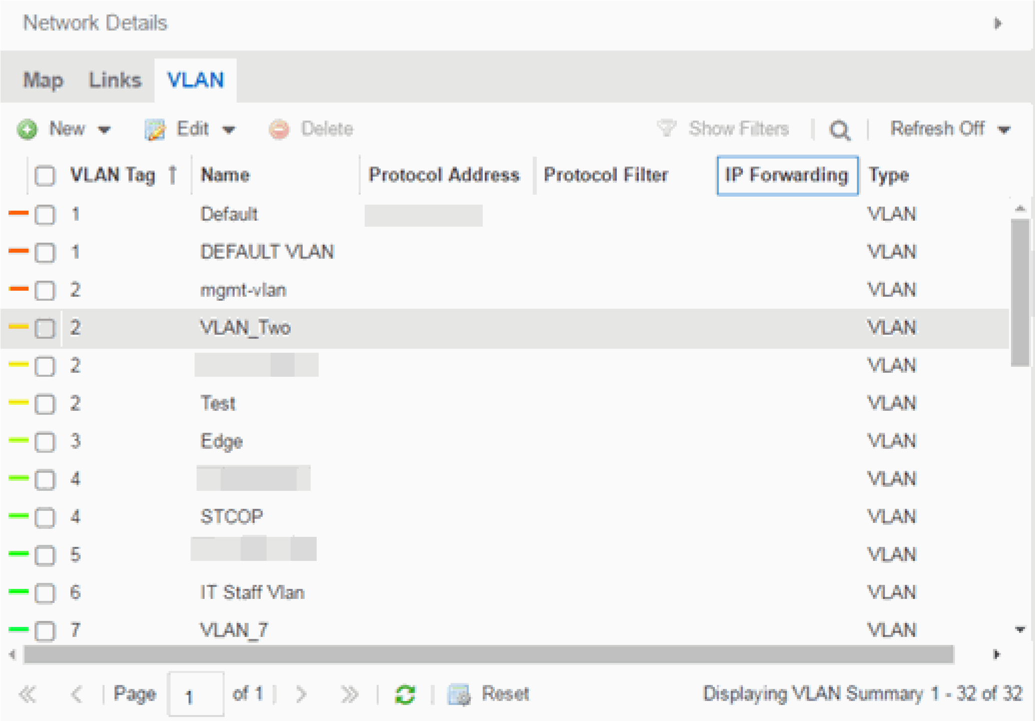
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down menu.
3. Select **VLAN Summary**.

NOTE: For an alternate way to access the VLAN Summary tab:

1. Click **Network > Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **VLAN** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

VLAN Summary tab

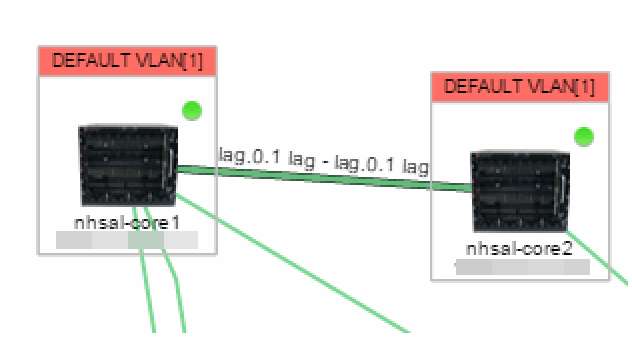
The **VLAN** Summary tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled for the VLAN.



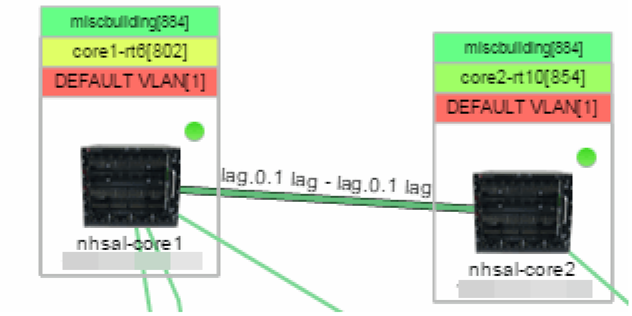
	□	VLAN Tag ↑	Name	Protocol Address	Protocol Filter	IP Forwarding	Type
🟧	□	1	Default	[redacted]			VLAN
🟧	□	1	DEFAULT VLAN				VLAN
🟧	□	2	mgmt-vlan				VLAN
🟨	□	2	VLAN_Two				VLAN
🟨	□	2	[redacted]				VLAN
🟨	□	2	Test				VLAN
🟩	□	3	Edge				VLAN
🟩	□	4	[redacted]				VLAN
🟩	□	4	STCOP				VLAN
🟩	□	5	[redacted]				VLAN
🟩	□	6	IT Staff Vlan				VLAN
🟩	□	7	VLAN_7				VLAN

Page 1 of 1 | Reset | Displaying VLAN Summary 1 - 32 of 32

Selecting the checkbox associated with a VLAN highlights any devices to which that VLAN is assigned by surrounding the device in a box with a color-coded title bar containing the VLAN name.



Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.



Additionally, from the **VLAN** tab, you can create a new VLAN or create a VLAN protected by an EAPS domain via the **New** drop-down menu. You can edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down menu.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the MLAG tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **MLAG** tab lists devices configured in a multi-switch link aggregation group.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

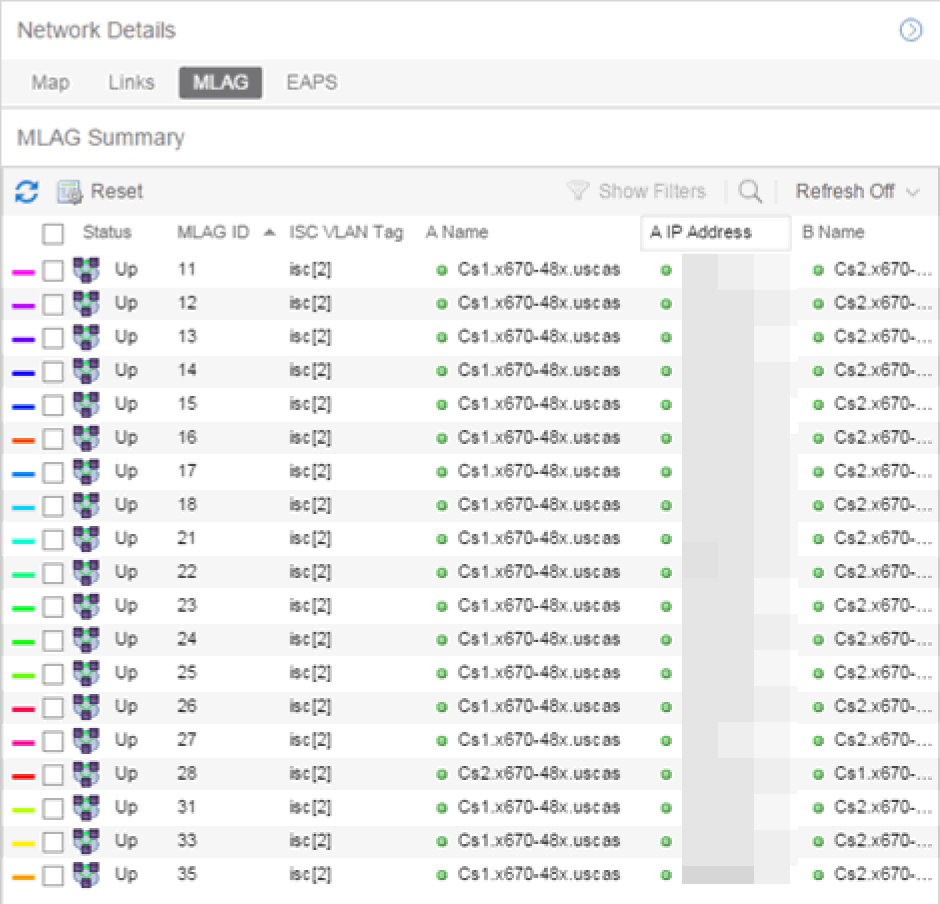
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down menu.
3. Select **MLAG Summary**.

NOTE: For an alternate way to access the MLAG Summary tab:

1. Click **Network > Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **MLAG** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

MLAG Summary tab

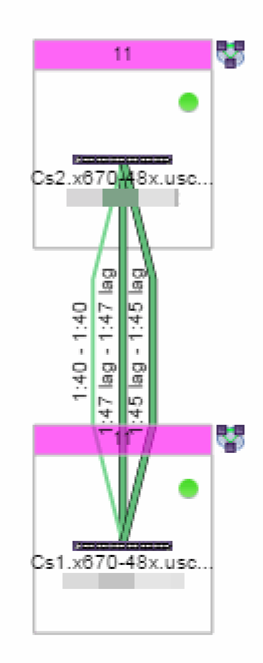
The **MLAG** Summary tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of the MLAG. Additionally, the Connected IP column displays the IP of the switch to which the MLAG is connected.



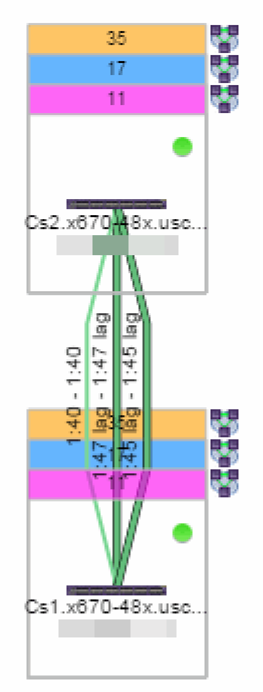
MLAG Summary

☐	Status	MLAG ID ▲	ISC VLAN Tag	A Name	A IP Address	B Name
☐	Up	11	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	12	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	13	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	14	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	15	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	16	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	17	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	18	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	21	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	22	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	23	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	24	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	25	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	26	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	27	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	28	isc[2]	● Cs2.x670-48x.uscas	● [redacted]	● Cs1.x670-...
☐	Up	31	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	33	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...
☐	Up	35	isc[2]	● Cs1.x670-48x.uscas	● [redacted]	● Cs2.x670-...

Selecting the checkbox associated with an MLAG highlights any devices containing ports associated with the MLAG by surrounding the device in a box with a color-coded title bar containing the MLAG ID.



Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.



Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the VPLS tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **VPLS tab** displays information about site connectivity within a private VLAN.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down menu.

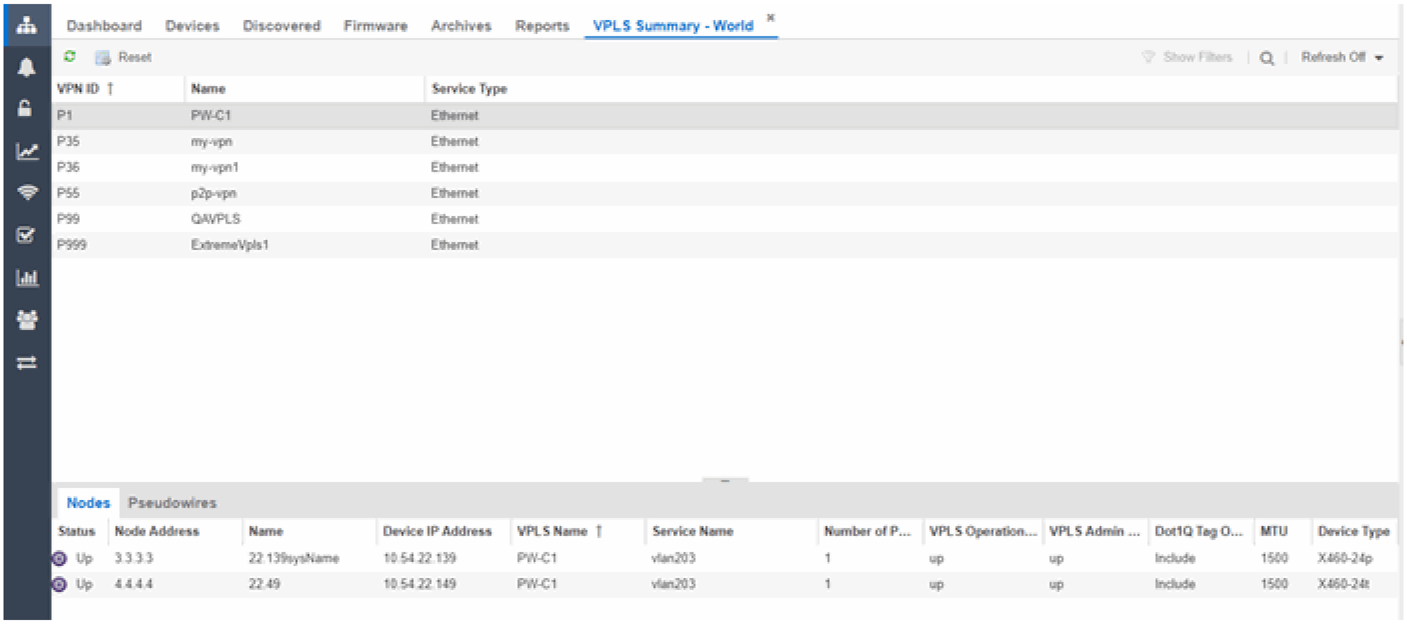
3. Select **VPLS Summary**.

NOTE: For an alternate way to access the VPLS Summary tab:

1. Click **Network > Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **VPLS** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

VPLS Summary Tab

VPLS Summary Tab provides information about the virtual private networks (VPNs) within a map. The tab displays the VPN ID, name and service type for each VPN in the map. In addition, the Nodes and Pseudowires (PW) tabs provide more detailed operational information specific to each VPN.



VPN ID ↑	Name	Service Type
P1	PW-C1	Ethernet
P35	my-vpn	Ethernet
P36	my-vpn1	Ethernet
P55	p2p-vpn	Ethernet
P99	QAVPLS	Ethernet
P999	ExtremeVpls1	Ethernet

Status	Node Address	Name	Device IP Address	VPLS Name ↑	Service Name	Number of P...	VPLS Operation...	VPLS Admin ...	Dot1Q Tag O...	MTU	Device Type
Up	3.3.3.3	22.139sysName	10.54.22.139	PW-C1	vlan203	1	up	up	Include	1500	X460-24p
Up	4.4.4.4	22.49	10.54.22.149	PW-C1	vlan203	1	up	up	Include	1500	X460-24t

Nodes

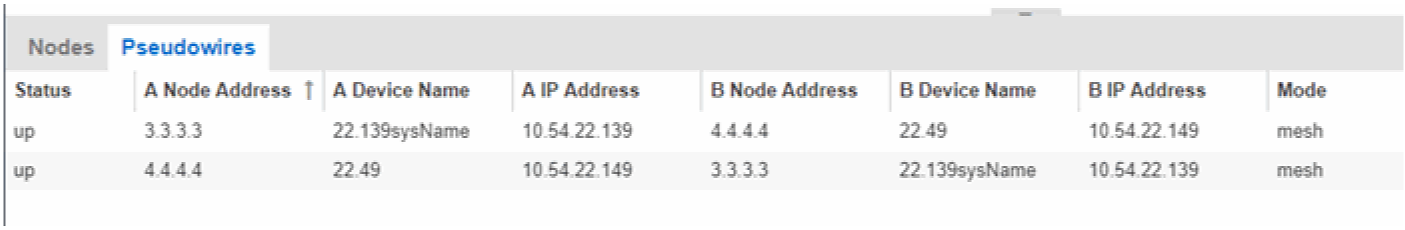
The **Nodes tab** includes the following:

- Status - operational status of the node
- Node Address - node location within the VPN
- Name - name of the node
- Device IP Address -

- VPLS Name - name of the VPLS in which the node resides
- Service Name - name of the virtual private LAN in which the node resides
- Number of Peers - number other nodes in the VPN
- VPLS Operational Status - operational status of the virtual private LAN services
- VPLS Admin Status - administrative status of the virtual private LAN services
- Dot1Q Tag Option -
- MTU - the maximum number of transmission units allowed between nodes
- Device Type -

Pseudowires

Click the **Pseudowires Tab** for access to the status and mode for each PW in the VPN, as well as the addresses, device names, and IP addresses for each node within the VPN.



Status	A Node Address ↑	A Device Name	A IP Address	B Node Address	B Device Name	B IP Address	Mode
up	3.3.3.3	22.139sysName	10.54.22.139	4.4.4.4	22.49	10.54.22.149	mesh
up	4.4.4.4	22.49	10.54.22.149	3.3.3.3	22.139sysName	10.54.22.139	mesh

Related Information

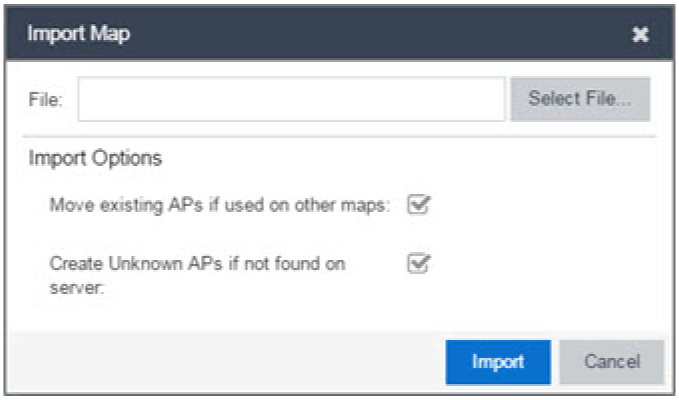
For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center Import Map

Use this window to import a saved map. From this window you can navigate to a saved map file and configure the behavior of the imported map.

Access this window by right-clicking a map in the Groups/Maps Navigation Tree left-panel on the **Network** > **Devices** tab, and selecting **Maps** > **Import Map**.



Import Map

File:

Import Options

Move existing APs if used on other maps: ☑

Create Unknown APs if not found on server: ☑

File

The file path to the saved map file. Click the **Select File** button to navigate to the file on your local drive or network.

Import Options

The Import Options section determines the behavior of APs on the map being imported.

Move existing APs if used on other maps

Select this checkbox to move APs currently located on another map in Extreme Management Center to the map being imported.

Create Unknown APs if not found on server

When this checkbox is selected, APs located on the map being imported not found on the Extreme Management Center server are created as unknown APs.

Related Information

For information on related topics:

- Maps Overview
- Maps
- How to Create and Edit Maps

Extreme Management Center Map Types

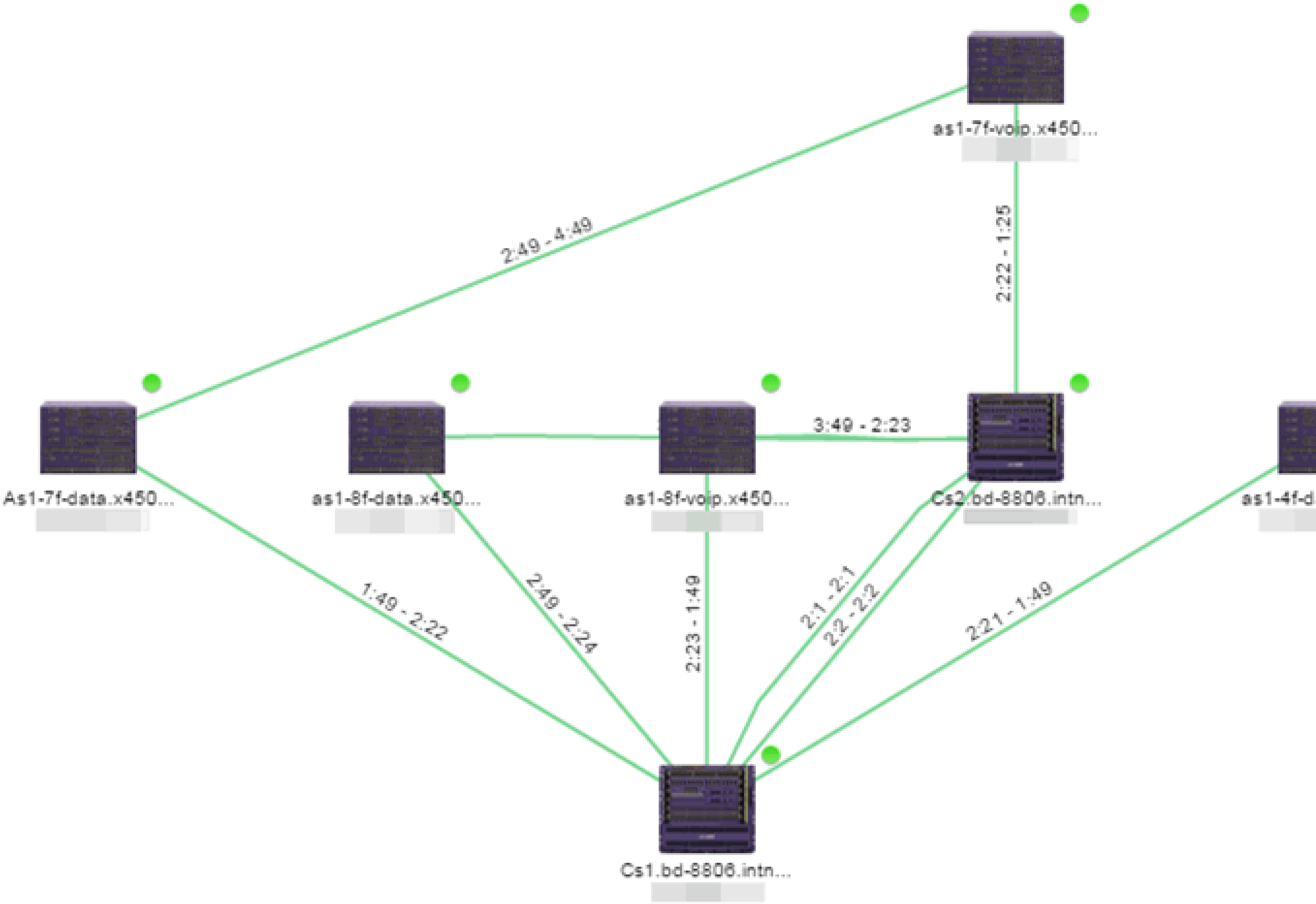
Extreme Management Center allows you to create geographic and topology maps of devices and floorplans of wireless access points (APs) on your network.

To view maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

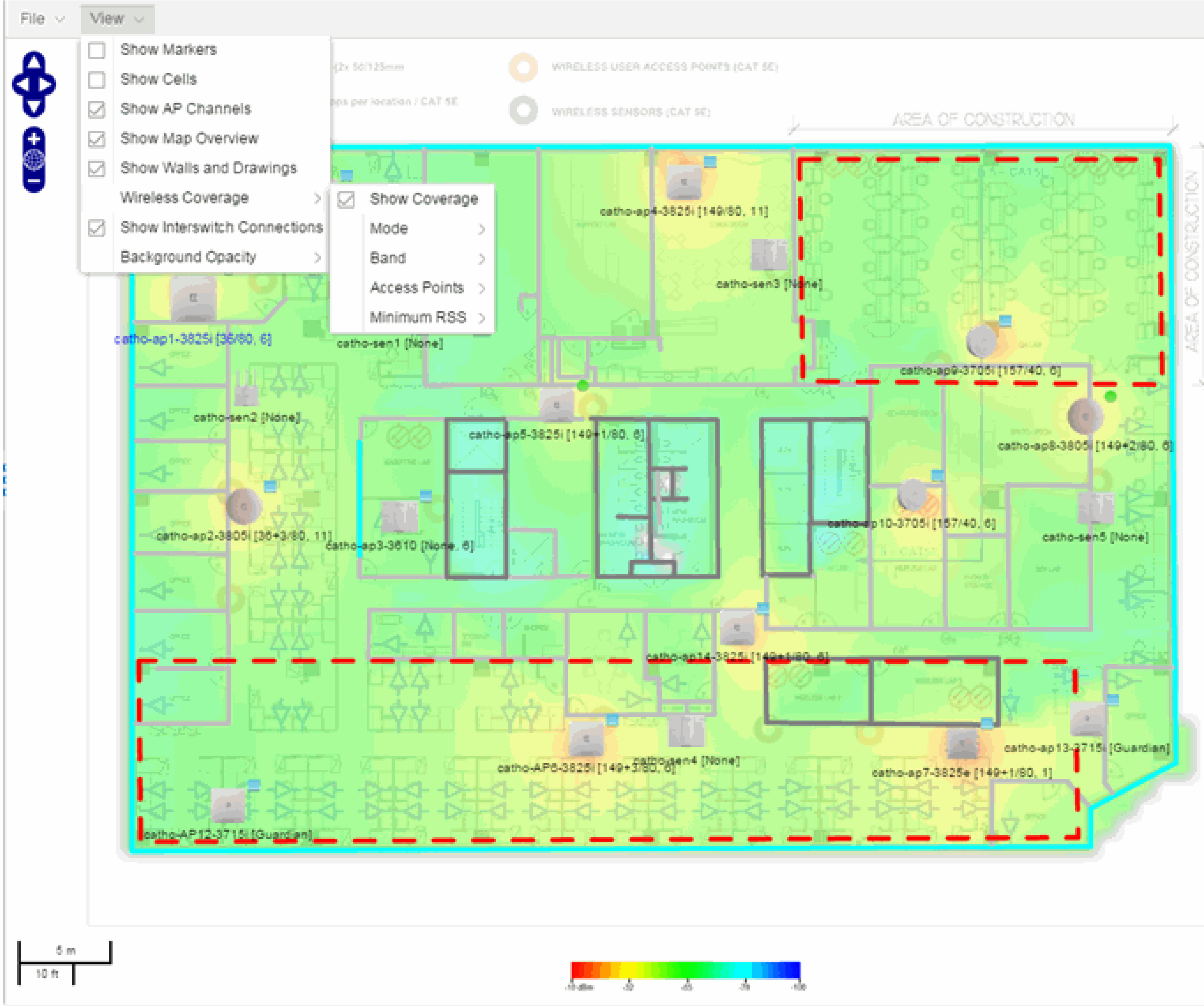
Types of Maps

Using Extreme Management Center Maps, you can create three types of maps, each presenting a different visual representation of your network:

- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.



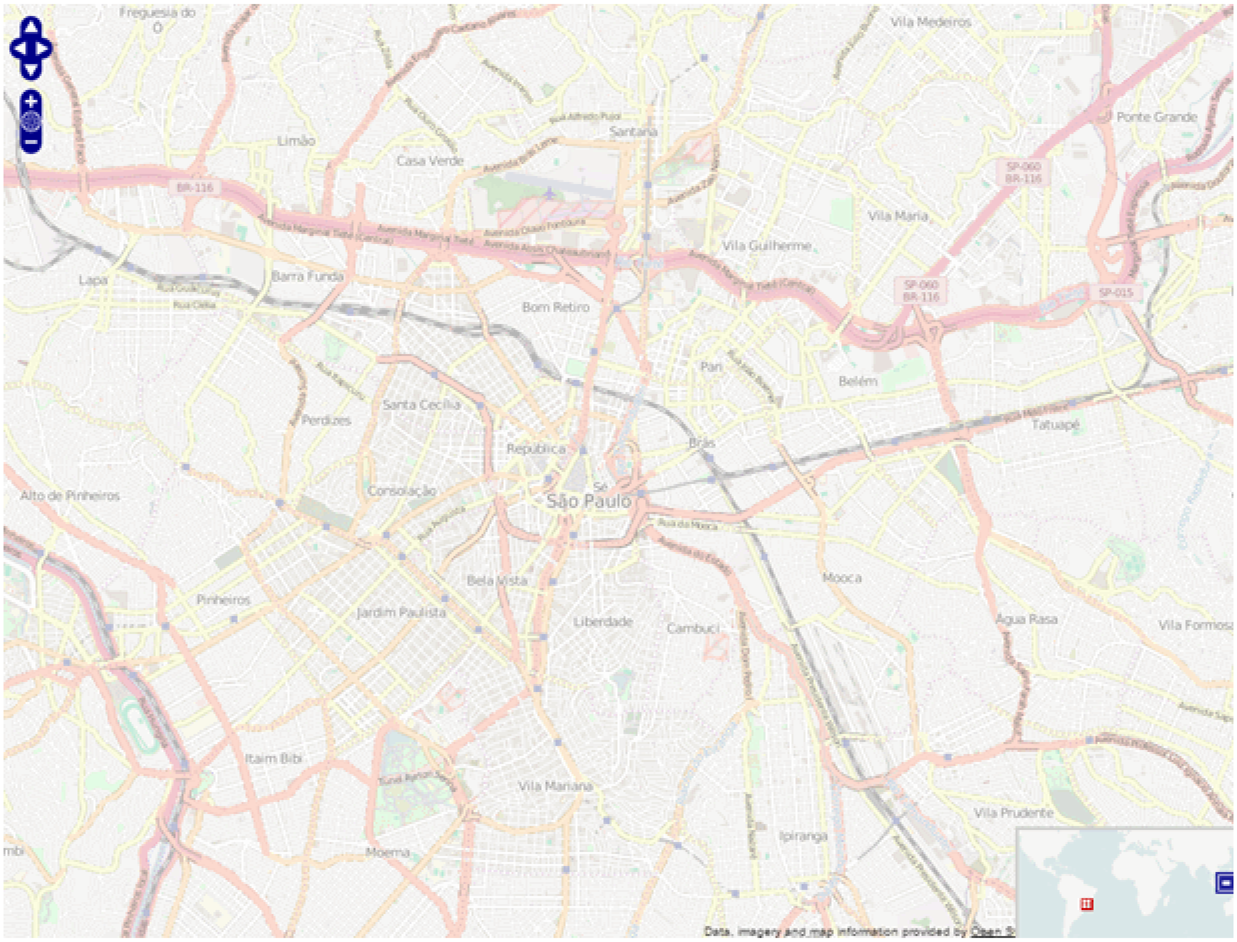
- Floorplan — The floorplan map displays the location of APs in a floorplan you configure. Using information about the size and composition of the building, this map provides an overview of the coverage of wireless APs.


File
View
□ Show Markers
□ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage >
☑ Show Interswitch Connections
Background Opacity >
☑ Show Coverage
Mode >
Band >
Access Points >
Minimum RSS >
AREA OF CONSTRUCTION
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-ap4-3825i [149/80, 11]
catho-sen3 [None]
catho-ap9-3705i [157/40, 6]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap8-3805i [149+2/80, 6]
catho-ap2-3805i [36+3/80, 11]
catho-ap3-3610 [None, 6]
catho-ap10-3705i [157/40, 6]
catho-sen5 [None]
catho-ap14-3825i [149+1/80, 6]
catho-AP6-3825i [149+3/80, 6]
catho-sen4 [None]
catho-ap7-3825e [149+1/80, 1]
catho-ap13-3715i [Guardian]
catho-AP12-3715i [Guardian]
5 m
10 ft

NOTE: The floorplan map type is only available with the NMS-ADV license.

- Geographic — The Geographic map shows a global or regional view where network locations are shown geographically. This map is useful for networks spread across large geographical areas or as a top-level map used to organize multiple networks in different locations.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



After you create a map, you can then make it a site. Sites allow you to set a default configuration for devices added to your network.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Perform a Search Using Extreme Management Center Maps

Using Extreme Management Center Maps, you can easily search for wireless and wired clients, access points (APs), and devices in a number of ways. Maps are configured in various places on the **Network** > **Devices** tab in Extreme Management Center.

Performing a Search

To search for a wireless client, an AP, a device, or a wired client:

1. Launch Extreme Management Center.
2. In the **Search Network** box, click **Advanced** .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information in the open **Search** box.
4. Press **Enter**.

You can also search for specific wireless clients, access points, devices, and wired clients from different locations in Extreme Management Center.

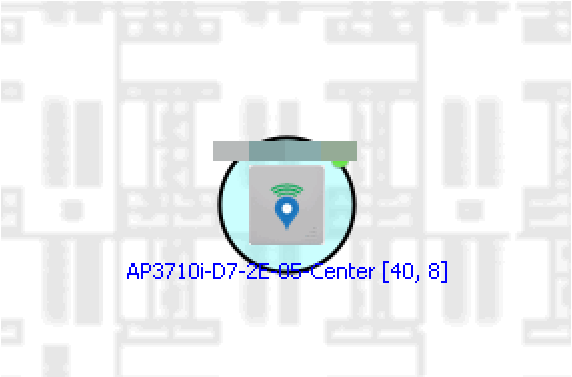
Finding a Wireless Client

From the Search Field on the Network Tab

1. Launch Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
3. Select the map or map navigation tree.
4. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information in the **Search** field at the far right of the **Devices** window.
5. Press **Enter**.

The search uses RSS-based (Received Signal Strength) location services to locate the wireless client and display the approximate location of the client on the map.

The map opens with the AP centered on the map, with a circle showing the possible area where the client is located. If that information is not available, a square is drawn around the AP last associated with the client.



From the Wireless Tab

To locate a wireless client from the Wireless tab:

1. Launch Extreme Management Center.
2. Click **Wireless > Clients.**
3. Select a client in the Clients view.
4. Right-click and select **Search Maps**.
5. The map opens centered on the AP, with a circle showing the possible area where the client is located.
6. Mouse over the client icon to see a tooltip with client information.

NOTE: Tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients page.

Radius Distance Calculation

The following distance calculation defines the radius of the circle displayed around the wireless client located on the map.

Path loss per meter in free space =
L1 = 20 * log (10) (f) - 28

where:

- [f] is the frequency in MHz
(Uses Source SNMP MIB dot11ExtSmtCurrentChannel
or if that value is 0, uses MIB dot11ExtSmtCurChanSelectedByAP)
- [L1] is the path loss on distance of 1 meter

Radial distance for location =
$d(RSS,n) = 10\,\hat{}\,(pTx - RSS - L1)/(10*n)$

where:

- [n] is the coefficient for the environment
- [pTx] is the transmit power (dB)
- [RSS] is the Received Signal Strength
- [d] is the distance in meters

Finding an Access Point

From the Wireless Tab

1. Launch Extreme Management Center.
2. Click **Wireless** > **Access Points.**
3. Right-click an AP in the table.
4. Select **Maps > Search Maps**.
5. If a map contains the AP, the map opens with the AP centered on the map.

From the Reports Page

1. Launch Extreme Management Center.
2. Click the **Wireless** tab.
3. On the **Reports** tab, click the APs Summary from the **APs Summary** drop-down menu.
4. Right-click an AP in the table.
5. Select **Maps > Search Maps**.
6. If a map contains the AP, the map opens with the AP centered on the map.

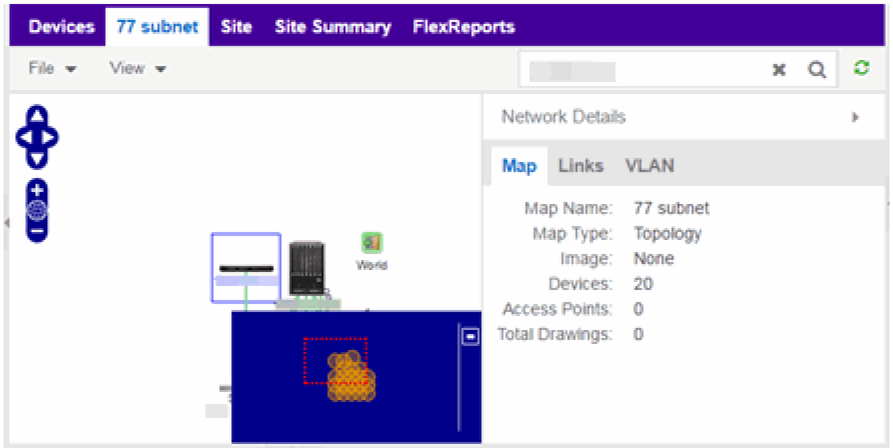
Finding a Device

From the Network Page Search Field

1. Launch Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
3. Select the map or map navigation tree. Click the **Map** tab in the **Devices** window.

4. Enter an IP address or hostname for the device in the **Network** tab **Search** box
5. Press **Enter**.

The search locates a device added to a map. The map centers on the device. The screen shot below shows the results for a search on a specific IP address.



Map Name: 77 subnet
Map Type: Topology
Image: None
Devices: 20
Access Points: 0
Total Drawings: 0

Finding a Wired Client

From the Network Tab Search Field

1. Launch Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
3. Select the map or map navigation tree.
4. Enter the MAC Address, IP Address, hostname, or user name in the **Network** tab **Search** box.
5. Press **Enter**.

The search locates a wired client if the client is Extreme Access Control authenticated and is connected to a switch added to a map. The map centers on the wired client.

From the Control Tab

1. Launch Extreme Management Center.
2. Click **Control** > **End-Systems.**
3. Right-click an end-system in the table and select **Search Maps**.

4. If the end-system is connected to a switch added to a map, the map opens with the end-system centered on the map.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

How to Import Maps

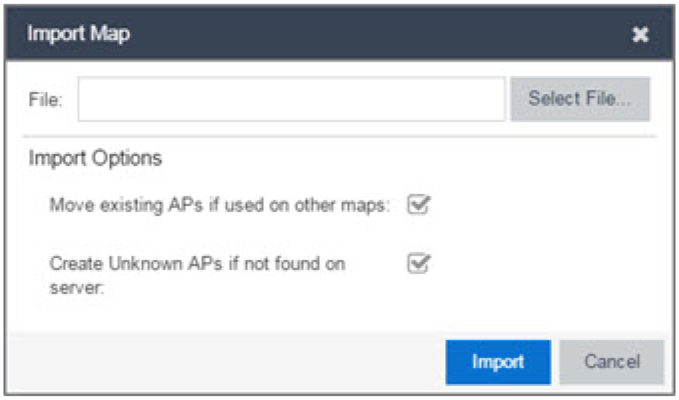
The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Importing a Map

To import a saved map:

1. Right-click a map in the left-panel Groups/Maps Navigation Tree and select **Maps** > **Import Map**.
   The Import Map window opens.



Import Map

File:

Import Options

Move existing APs if used on other maps: ☑

Create Unknown APs if not found on server: ☑

2. Click the **Select File** button to navigate to the map on your local drive or network.

3. Configure your import options to determine the behavior of APs on the map being imported:
    a. Select the **Move existing APs if used on other maps** checkbox to move APs currently located on another map in Extreme Management Center to the map being imported.
    b. Select the **Create Unknown APs if not found on server** checkbox for APs located on the map being imported that are not found on the Extreme Management Center server.
4. Click **Import**.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Create Links Between Devices and Maps

Using the Extreme Management Center Maps feature, you can link your network devices and wireless access points (APs) on a map. You can also use this feature to add links between maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Creating a Manual Link Between Devices

To manually create links between devices on a map:

1. Right-click one of the devices to which you are adding the link.
2. Select **Create Link**.

    The Create a Manual Link window displays.
3. Expand the device in the **Name** column of the From Port section of the window and select the port to which the link connects.
4. Select the other device to which the link connects in the **Select Device** drop-down menu.

5. Expand the device in the **Name** column of the To Port section of the window and select the port to which the link connects.
6. Click **OK** to add the link to the map.

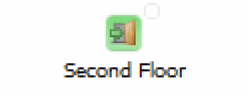
NOTES: The **Link State** for a manual link is derived from the **Status** of the ports to which it connects.

Delete a manual link via the Link Details window by double-clicking the link in the map.

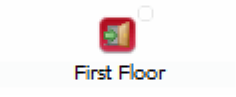
Adding Map Links

Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating there are no devices with alarms on the Second Floor map.



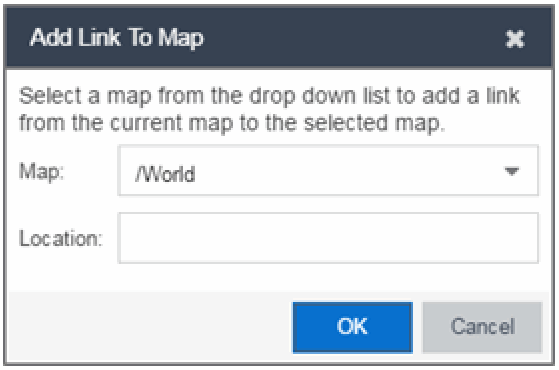
The following map link lets you jump to the First Floor map. The link is red, indicating there is an alarm for a device on the First Floor map.



Use the following steps to add a link to a map.

1. In the Maps navigation tree, right-click on the map from which you want to link and select **Maps** > **Edit Map** or click **File** > **Edit** button in the map properties panel.
2. The map's property panel opens in Edit mode. Click **File** > **Add** > **Map Link**.

3. The **Add Link to Map** window opens.



Select a map from the drop down list to add a link from the current map to the selected map.

Map: /World

4. From the **Map** drop-down menu, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and click **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Click the **Save** button to save the map and close the properties panel.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Set the Map Scale

You can use the Extreme Management Center Maps feature to set the scale of a map of devices or wireless access point (APs) in your network.

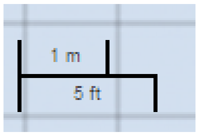
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

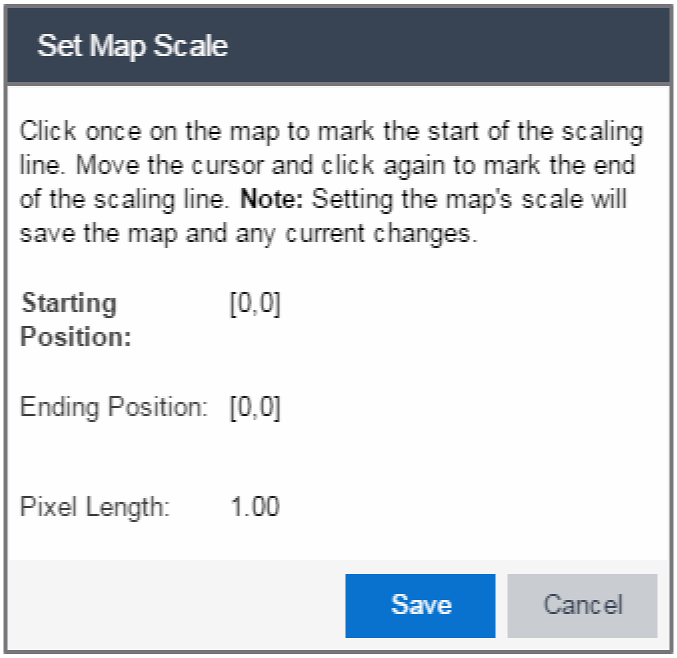
Setting the Map Scale

The map scale appears in the lower left corner of a map and can be changed to accurately reflect your map image.

Use the following steps to set the scale for a map.

1. In the Maps page's navigation tree, right-click on the map and select **Maps** > **Edit Map** or click the **File** > **Edit** button in the map properties panel.
2. Click on the map scale in the map's footer panel to open the Set Map Scale window. (Users with the Extreme Management Center NMS-ADV license can access the Set Map Scale window from the Tools menu.)





Set Map Scale

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. **Note:** Setting the map's scale will save the map and any current changes.

Starting Position: [0,0]

Ending Position: [0,0]

Pixel Length: 1.00

3. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floor plan, measure a scaling line on the opening of an office. If you know the office doors are 33 inches wide, enter that as the scaling line measurement.
   a. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
   b. Enter the line length and units.
4. Click **Save**. The map scale is automatically adjusted and the map is saved.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center Restart Devices

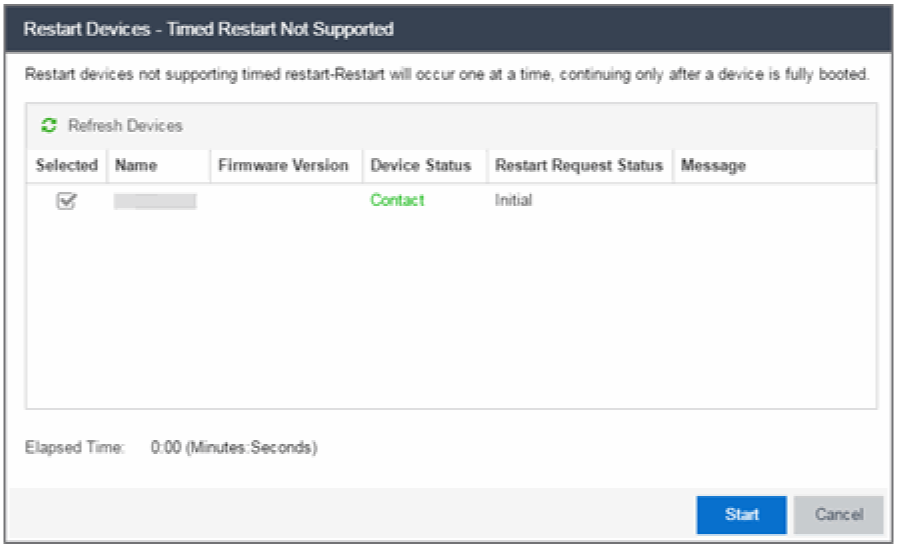
Use this window to restart a device. Devices can be restarted manually, or scheduled at a future date and time, if a timed restart is supported by the device. The window varies depending on the devices you select to restart:

- Timed Restart Not Supported
- Timed Restart Supported

You can access the Restart Devices window from the Network tab by clicking the **Menu** icon or right-clicking a device in the table and selecting **Configuration/Firmware** > **Restart Device**.

Timed Restart Not Supported

To restart a device, select it in the list by clicking the **Selected** checkbox, and click **Start**.



Restart Devices - Timed Restart Not Supported

Restart devices not supporting timed restart-Restart will occur one at a time, continuing only after a device is fully booted.

Selected	Name	Firmware Version	Device Status	Restart Request Status	Message
☑	[redacted]		Contact	Initial	

Elapsed Time: 0:00 (Minutes:Seconds)

Refresh Devices

Click the **Refresh Devices** button to update the fields in this window as the restart process is taking place.

Selected

Select this check box to indicate the devices you are restarting.

Name

The names of the devices.

Firmware Version

The firmware version of the devices. If the purpose of the device restart is to upgrade the firmware version, this value changes once the device restart is complete (update the field by clicking **Refresh Device**).

Device Status

The connection status between Extreme Management Center and the devices.

Restart Request Status

The time in the restart process during which the devices indicate they are restarting.

Message

Additional information about the devices.

Elapsed Time

The time elapsed since the restart began.

Start

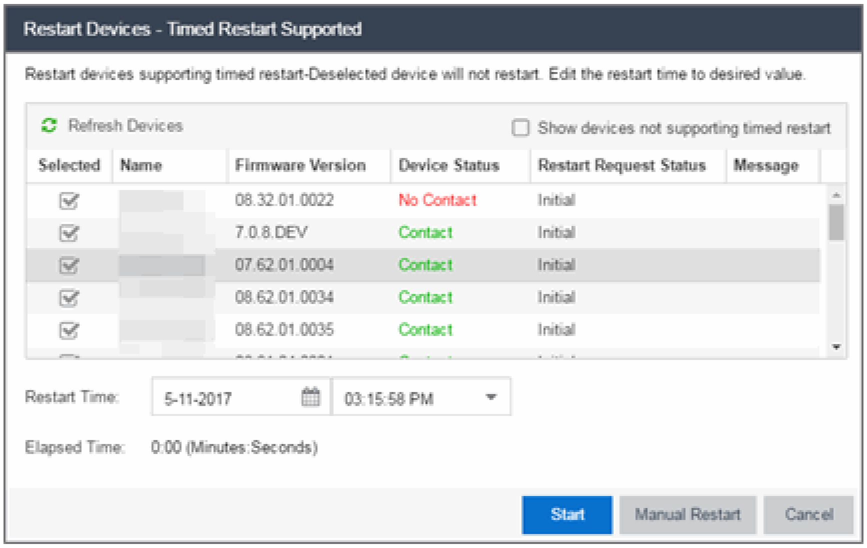
Click **Start** to restart the device.

Close

Click **Close** to exit the **Restart Devices** window without restarting the devices.

Timed Restart Supported

Devices that support Timed Restart allow you to set up your restart operation with a time delay, so that the actual device restarts take place at a later time. This lets you schedule restarts for a time when the network is least busy.



Restart Devices - Timed Restart Supported

Restart devices supporting timed restart-Deselected device will not restart. Edit the restart time to desired value.

Refresh Devices □ Show devices not supporting timed restart

Selected	Name	Firmware Version	Device Status	Restart Request Status	Message
☑	[redacted]	08.32.01.0022	No Contact	Initial	
☑	[redacted]	7.0.8.DEV	Contact	Initial	
☑	[redacted]	07.62.01.0004	Contact	Initial	
☑	[redacted]	08.62.01.0034	Contact	Initial	
☑	[redacted]	08.62.01.0035	Contact	Initial	

Restart Time: 5-11-2017 03:15:58 PM

Elapsed Time: 0:00 (Minutes:Seconds)

The window for these devices contains additional fields.

Refresh Devices

Click the **Refresh Devices** button to update the fields in this window as the restart process is taking place.

Selected

Select this check box to indicate the devices you are restarting.

Name

The names of the devices.

Firmware Version

The firmware version of the devices. If the purpose of the device restart is to upgrade the firmware version, this value changes once the device restart is complete (update the field by clicking **Refresh Device**).

Device Status

The connection status between Extreme Management Center and the devices.

Restart Request Status

The time in the restart process during which the devices indicate they are restarting.

Message

Additional information about the devices.

Elapsed Time

The time elapsed since the restart began.

Start

Click this button to schedule the device restart now, or at the time selected in the Restart Time field.

Close

Click this button to exit the Restart Devices window without restarting the devices.

Show devices not supporting timed restart

Select this check box to display devices you selected on the Network tab for which you can not schedule a restart.

Restart Time

Select the date and time when the devices restart.

Related Information

For information on related topics:

- How to Restart a Device

How to Create an EAPS Domain in Extreme Management Center

This section outlines how to create an EAPS domain, from the Network tab.

To create a new EAPS Domain:

1. Launch Extreme Management Center.
2. Open the **Network** > **Devices** tab and select a map within the World map navigation tree.
3. Click the EAPS tab in the Network Details section of the window. The EAPS Summary pane opens.
4. Click the **New EAPS Domain** button. The New EAPS Domain wizard opens to the Select Devices window.
5. Highlight the devices to add to the EAPS domain and click the right arrow button to move the devices to the selected device column.

   NOTE: Use the up and down arrows to change the order in which devices are listed.

6. Click **Next >**. The Configure Domain window opens.
7. Enter a **Name** for the EAPS domain.
8. Select the links to add to the EAPS domain in the Available Links section and click the **Add** button.
9. Enter the **Name** and **Tag** of the Control VLAN for the EAPS domain.
10. Select a **Master Node** and **Primary Port** for the EAPS domain from the drop-down menus in the Master Node section of the window.
11. Enter the amount of time, in seconds, for the **Hello** and **Fail** timers.
    - **Hello Timer** — The interval, in seconds, between which polling signals are sent by the master node to detect ring breaks.
    - **Fail Timer** — The amount of time, in seconds, after the master node sends the Hello Timer signal until the master node detects a ring failure if a reply signal is not received. If a ring failure occurs, the switch can respond by either sending an alert or opening the secondary port.

1. Click **Next >**. The Results window opens.
2. Verify the EAPS domain is properly created.

   NOTE: If the EAPS domain is not created correctly, click the **< Back** button to change the values in the New EAPS Domain wizard.

3. Click **Close** to exit the New EAPS Domain wizard. The EAPS domain is created.

Related Information

For information on related topics:

- Maps
- Network
- How to Create and Edit a VLAN

Extreme Management Center VLAN Concepts

The following concepts will assist you in configuring VLAN and port template definitions in Extreme Management Center.

Information on:

- Egress Rules (Transmitting Frames)
    - Dynamic Egress
        - GVRP
        - GARP Timers
- Enforcing
- Frame Types
- IGMP
    - Interface Robustness (Robustness Variable)
    - Last Member Query Interval
    - Query Interval
    - Query Response
- Ingress Filtering
- Priority Classification
    - Weighted Priority
- Verifying
- VLAN Identification
    - Port VLAN ID (PVID)
    - VLAN ID (VID)
- VLAN Model
- VLAN Learning

Egress Rules (Transmitting Frames)

A device determines which frames can be transmitted out a port based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames. You can add or remove ports to or from a VLAN's Egress List, thereby controlling which VLAN's frames can be forwarded out which ports.

When a frame is transmitted out a port, the device first checks the Egress List. If the port is listed on the Egress List of the VLAN associated with it, the frame is then transmitted according to the priority assigned to the frame. The frame is transmitted as tagged or untagged according to the specification in the Egress List. If the port is not on the Egress List, or if the port is not operational, the frame is discarded.

Dynamic Egress

In Extreme Management Center, you can control whether or not Dynamic Egress is enabled for a VLAN in the VLAN Definitions table. When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means that you do not need to add the ingress port to the VLAN's egress list manually. (See Example 1, below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. In the Port Template Definitions view, you can enable GVRP (GARP VLAN Registration Protocol), which automatically adds the interswitch ingress ports to the egress lists of VLANs. (See Example 2, below.)

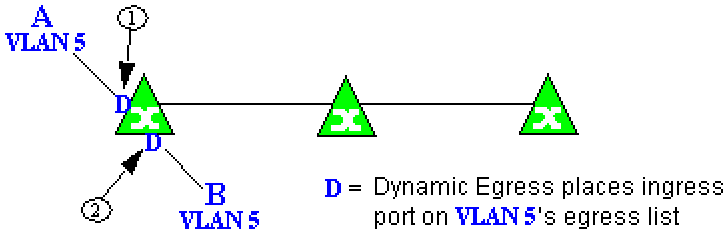
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

If an endstation is talking to a "silent" endstation which does send responses, like a printer, you will need to add the silent endstation's ingress port to the VLAN's egress list manually with a tool like NetSight Device Manager, or local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See Example 4, below.)

CAUTION: If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries will time out. The result is that an endstation will appear "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A & B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A will not be able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

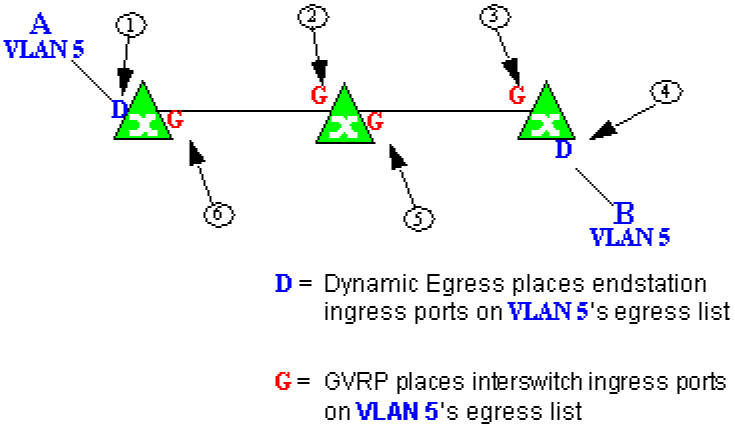
Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.


A
VLAN 5
1
D
D
2
B
VLAN 5
D = Dynamic Egress places ingress port on VLAN 5's egress list

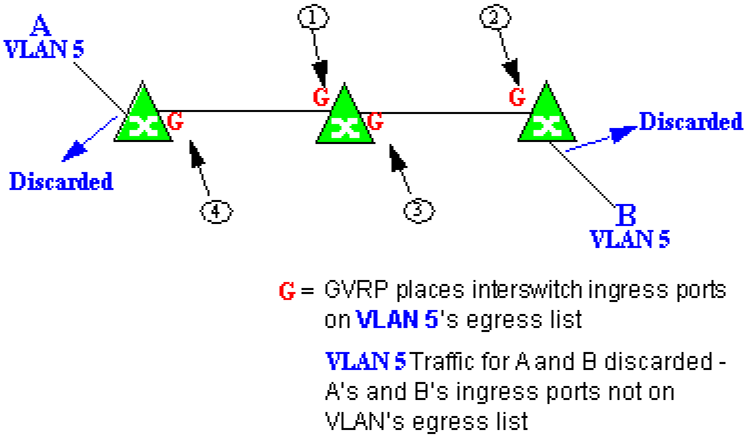
Example 2: Dynamic Egress + GVRP

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.


A
VLAN 5
1
2
3
4
D
G
G
G
G
D
6
5
B
VLAN 5
D = Dynamic Egress places endstation ingress ports on VLAN 5's egress list
G = GVRP places interswitch ingress ports on VLAN 5's egress list

Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.


A
VLAN 5
1
2
G
G
G
G
Discarded
Discarded
4
3
B
VLAN 5
G = GVRP places interswitch ingress ports on VLAN 5's egress list
VLAN 5 Traffic for A and B discarded - A's and B's ingress ports not on VLAN's egress list

Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.

GVRP

GVRP (GARP VLAN Registration Protocol) dynamically adds interswitch ingress ports to the egress lists of VLANs across a domain. You can enable and disable GVRP in the Port Template Definitions view.

NOTE: If you do not want GVRP enabled on your network, you can disable it, then manually configure the interswitch ports to do what GVRP does automatically, using MIB Tools or local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration.

GARP Timers

In the Port Template Definitions view, you can set GARP timers on the device to control the timing of dynamic VLAN membership updates to connected devices. The timer values must be identical on all connected devices in order for GVRP to operate successfully.

- Join Time - Frequency of messages issued when a new port has been added to the VLAN. Possible values are 1 through 1488800 milliseconds.
- Leave Time - Frequency of messages issued when a single port no longer belongs to the VLAN. This value must be at least three times greater than the Join Time. Possible values are 1 through 1488800 milliseconds.
- Leave All Time - Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. This value must be greater than the value for Leave Time. Possible values are 1 through 1488800 milliseconds.

Enforcing

When working with VLANs in NetSight Console, you can write the definitions in the VLAN model to selected devices or ports by clicking the **Enforce** button on the Device or Advanced Port view of the right panel VLAN tab in Console's main window. You can also enforce changes to individual ports on the Basic Port view of the VLAN tab in Console's main window. A green exclamation point ! in a table indicates that the setting will be written to the device when you enforce. Only those VLANs which have the Write VLAN to Devices box checked on the VLAN Properties tab are enforced. A verification is done automatically after the enforce is complete. A red ❌ appears if the enforcing of a particular setting fails.

NOTE: On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS_L3_ Interface Name). However, you can update a VLAN model definition with the System Static VLAN definition from the router.

Frame Types

Incoming frames are processed according to ingress rules which determine the VLAN membership and transmission priority of a frame received on a port by checking for the presence of a VLAN tag. A VLAN tag is a field within a frame that identifies the frame's VLAN membership and priority.

Frames can be tagged or untagged. A tagged frame is a frame that contains a VLAN tag. An untagged frame does not have a VLAN tag, but will be tagged when it is received on a port. A tagged frame may have already been processed by an 802.1Q switch or originated at an endpoint capable of inserting a VLAN tag into a frame. A VLAN tag may or may not contain a VLAN ID (VID), but it will always contain priority information. End systems are allowed to transmit frames with only a priority in the VLAN tag. When switches transmit a tagged frame, the VLAN tag will always include a VID along with the priority.

Tagged and untagged frames are assigned VLAN membership and transmission priority differently:

Untagged Frame - VLAN Membership

When an untagged frame is received on a port, if a VLAN Classification rule exists for the frame's classification type, the frame will gain membership in the associated VLAN. If not, the frame will be assigned to the VLAN identified as the port's VLAN ID (PVID).

Untagged Frame - Priority Assignment

When an untagged frame is received on a port, if a Priority Classification rule exists for the frame's classification type, the frame will be assigned the associated priority. If not, the frame will be assigned the port's default priority.

Tagged Frame - VLAN Membership

If a tagged frame includes a VID (VLAN ID), it will gain membership in the VLAN indicated by the VID. If not, and a VLAN Classification rule exists for the frame's classification type, the frame will be put into the associated VLAN. If there is no VID or classification rule, the frame will be put in the VLAN associated with the port's VLAN ID (PVID).

Tagged Frame - Priority Assignment

When a tagged frame is received on a port, it is assigned the priority contained in the VLAN tag.

You can set the acceptable frame type for a port on the Port Template Definitions view.

IGMP

IGMP (Internet Group Management Protocol) is a protocol used by IP hosts and their immediate neighbor multicast agents to support the allocation of temporary group addresses and the addition and deletion of members of a VLAN. You can enable and disable IGMP on the VLAN Definitions view.

IGMP Intervals

You can control the following IGMP query settings on the VLAN Definitions view:

- Query Interval - Interval (in seconds) between general IGMP queries sent by the device to solicit VLAN membership information from other devices. By setting this interval, you can control the number of IGMP messages on a subnet. Larger values cause queries to be sent less often. The Query Interval must be greater than the Query Response interval. Valid values: 1 through 300 seconds.
- Query Response - Maximum amount of time allowed for responses to general IGMP queries. By setting this value, you can control the burstiness of IGMP messages on a subnet. Larger values result in less bursty traffic, because host responses are spread over a larger interval. This value must be less than the Query Interval. Valid values: 1 through 300.
- Interface Robustness (Robustness Variable) - Indicates the susceptibility of the subnet to lost packets. If a subnet is particularly susceptible to losses, you may wish to increase this value. IGMP is robust to (Robustness Variable-1) packet losses. The

Interface Robustness value is used in the calculation of IGMP message intervals. Valid values are 2 thru 32767.

- **Last Member Query Interval** - Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. By setting this value, you can control the "leave latency" of the network. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds.

Ingress Filtering

Ingress Filtering is a means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame. For example, if a tagged frame with membership in the Sales VLAN is received on a Port 1, and Ingress Filtering is enabled, the switch will determine if the port is on the Sales VLAN's Egress List. If it is, the frame can be processed. If it is not, the frame is dropped. You can set ingress filtering for a VLAN on the Port Template Definitions view.

Priority Classification

Priority Classification is used to assign frames transmission priority over other frames. Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority.

Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

Frames can be assigned a transmission priority ;based on the default priority of the receiving switch port, regardless of the frame's classification type. However, with the addition of classification rules, frames can be assigned a priority based on the frame's classification type. Using priority classification rules, network administrators can classify a frame based on Layer 2/3/4 information to have higher or lower priority than other frames on a per port basis, allowing for better defined Class of Service configurations.

You can set the default priority for incoming frames on the Port Template Definitions view.

Weighted Priority

Weighted priority, available on certain devices, is a way to further refine priority classification. You can control this setting on the Port Template Definitions view.

Some devices support four transmit queues (0-3) per port. These queues can be serviced based on a strict method, meaning that all frames in Queue 3 will be transmitted before the frames in Queue 0, or based on a fair weighted method. The weighted method allows the network administrator to give a certain percentage or weight to each queue, preventing a lower priority queue from being starved.

Forwarding priority can be tuned to allocate a percentage of a port's transmit resources to the each traffic queue. This lets you adjust a strict priority scheme to guarantee that some percentage of frames from lower priority queues will always be sent. Weighted priority settings divide each port's transmit resources into 16 equal parts, which can be allocated to traffic queues in increments of 6.25% (1/16th). The total resource allocation for a port must always add up to 100%.

To understand the effect of weighted priorities, consider a device port with strict priority settings. In this case, all of the frames from the highest priority traffic queue are sent before frames are sent from any of the lower priority queues. Now, assuming four traffic queues, assign weighted priorities for the port giving 50% of the transmit resources to Queue 3, 25% to Queue 2, and 25% to Queue 1 and 0% to Queue 0. With these settings, at least 50% of the frames will be transmitted from Queue 3, at least 25% from Queue 2, at least 25% from Queue 1 and frames will only be transmitted from Queue 0 when Queue 1, 2, and 3 are empty.

Verifying

Verifying retrieves the VLAN settings on the selected devices and compares them with the settings in the selected VLAN Definitions view or Port Template Definitions view. This is done by way of the **Start Verify (Retrieve)** button ▶ on the Device or Advanced Port view of the VLAN tab in Console's main window. (In the Basic Port view of the VLAN tab in Console's main window, the ▶ button simply retrieves port VLAN information from the selected devices to populate the table.)

Only those VLANs which have the Write VLAN to Devices box checked on the VLAN Definitions view are compared. Differences are indicated by a red not-equals symbol ≠ in the device or ports table on the VLAN tab in Console's main window. A green exclamation point ! is displayed when you select a ≠ line in the table to the model setting that will be written to the device when you enforce. You can review the differences and make modifications to your model as needed, including updating the definitions in your model using the definitions from the selected devices (for VLAN Definitions) or ports (for Port Template Definitions).

For more information, see How to Work with VLAN Models.

VLAN Identification

VLAN identifiers include VLAN ID's and Port VLAN ID's.

VLAN ID (VID)

802.1Q VLANs are defined by VLAN IDs (VIDs) and VLAN names.

VID

A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VLAN Name

An alphanumeric name associated with a VLAN ID, used to make VLANs easier to identify and remember (up to 64 characters).

PVID (Port VLAN ID)

You can change a port's VLAN membership to reflect the specific needs of your network by assigning new VLAN membership to the port. When you assign VLAN membership to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port and the port is added to the VLAN's Egress List.

PVID

The PVID (Port VLAN ID) represents a port's VLAN assignment. Possible values are 1 through 4094.

Egress List

The Egress List specifies which ports can transmit the frames associated with the VLAN.

NOTE: On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

VLAN Model

NetSight Console enables you to create VLAN models and enforce them across multiple network devices. A VLAN model consists of at least one VLAN Definition and one VLAN Port Template, which you can define on the VLAN Definitions view and the Port Template Definitions view.

NetSight Console provides you with one VLAN model (the Primary VLAN Model) which is pre-populated with a Default VLAN (VID 1). You can further define this VLAN model, and/or you can create other VLAN models. (The Default VLAN for a model cannot be deleted.)

Once a VLAN model has been created, you can utilize it in the following ways:

- Use the Basic Port View of the VLAN tab in Console's main window to enforce the properties of a port template on selected devices. You can also make custom edits for selected ports using this view of the VLAN tab in Console's main window.
- Use the Device or Advanced Port view of the VLAN tab in Console's main window to perform a more detailed analysis of the differences between the definitions in the VLAN model and the VLAN settings on selected devices and their ports. Using these views of the VLAN tab in Console's main window, you can review the differences and make modifications to your VLAN model and/or device or port VLAN configuration as required, including updating any or all of the definitions in the model with the settings on selected devices and their ports, and writing (enforcing) a model's VLAN definitions and/or VLAN port templates to selected devices or ports.

See How to Work with VLAN Models for more information.

VLAN Learning

VLAN learning allows the creation of groups of VLANs that will share Filtered Database information (MAC address, port, and VLAN ID) according to 802.1Q Shared Learning Constraints (IEEE Std 802.1Q-1998). This helps to speed MAC to port lookups and reduce flooding, because MAC addresses will be in the same Filtering Database.

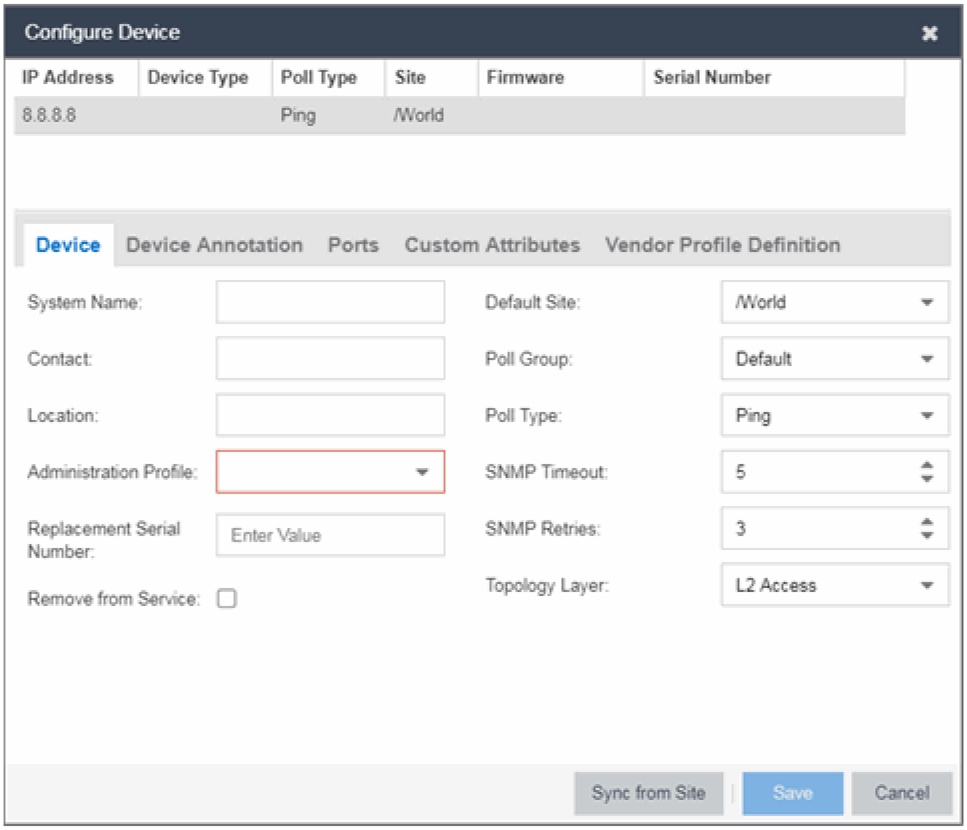
How to Create and Edit a VLAN in Extreme Management Center

This section outlines how to create and edit a VLAN. From the Network tab, you can:

- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

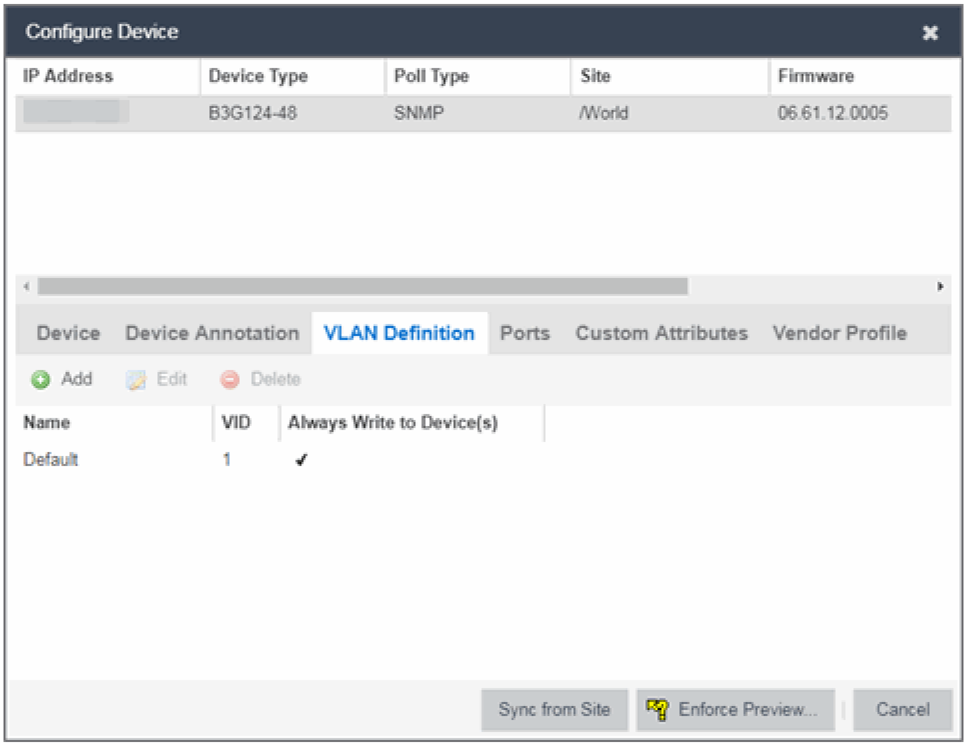
1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.



IP Address	Device Type	Poll Type	Site	Firmware	Serial Number
8.8.8.8		Ping	/World		

System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	□	Topology Layer:	L2 Access

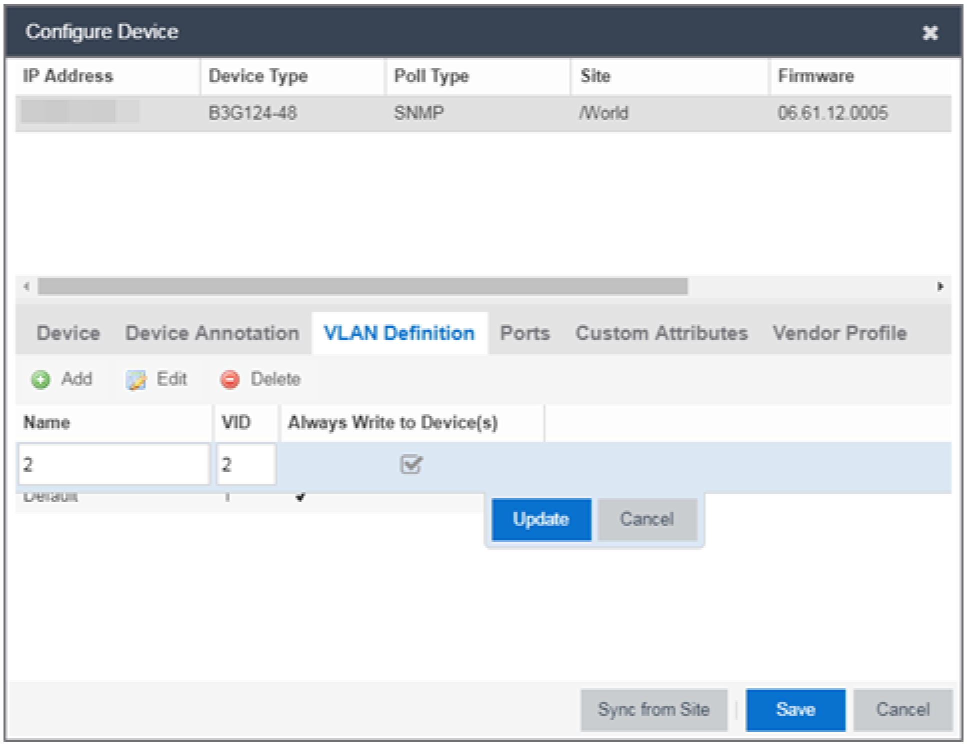
4. Select the **VLAN Definition** tab.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

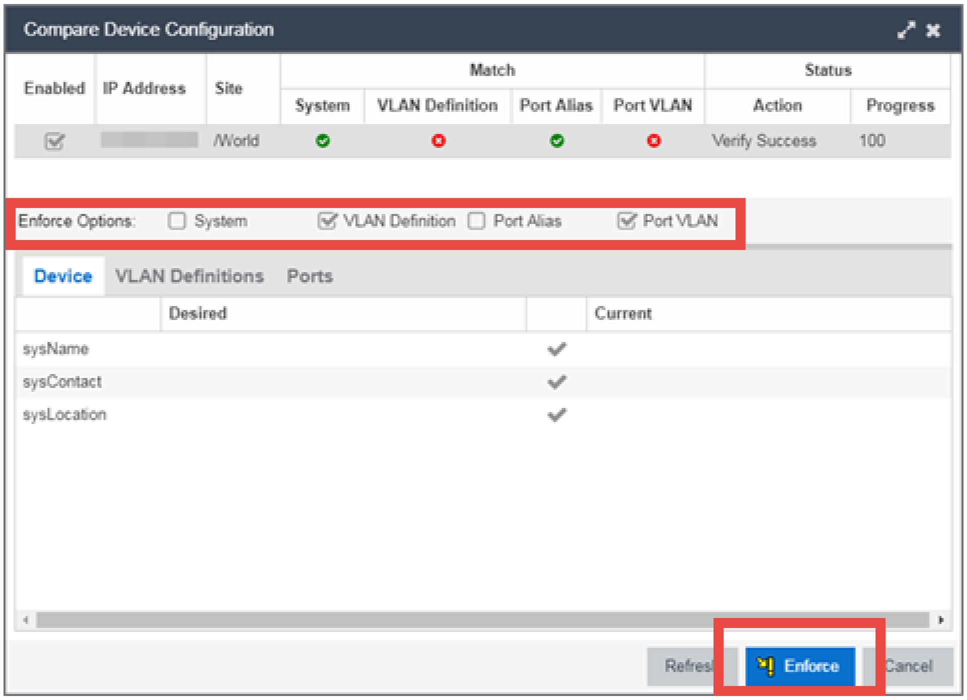
5. Click the **Add** button.
6. Enter the **Name** and the VID for the new VLAN.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
2	2	☑
Default	1	✓

7. Select **Update**.
   The new VLAN is added to the list.
8. Select **Enforce Preview**.
9. Under the Enforce Options, select the **VLAN Definition** checkbox and select **Enforce**.



Enabled	IP Address	Site	Match				Status	
			System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
☑	[redacted]	/World	🟩	🟥	🟩	🟥	Verify Success	100

Enforce Options: □ System ☑ VLAN Definition □ Port Alias ☑ Port VLAN

	Desired		Current
sysName		✓	
sysContact		✓	
sysLocation		✓	

NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

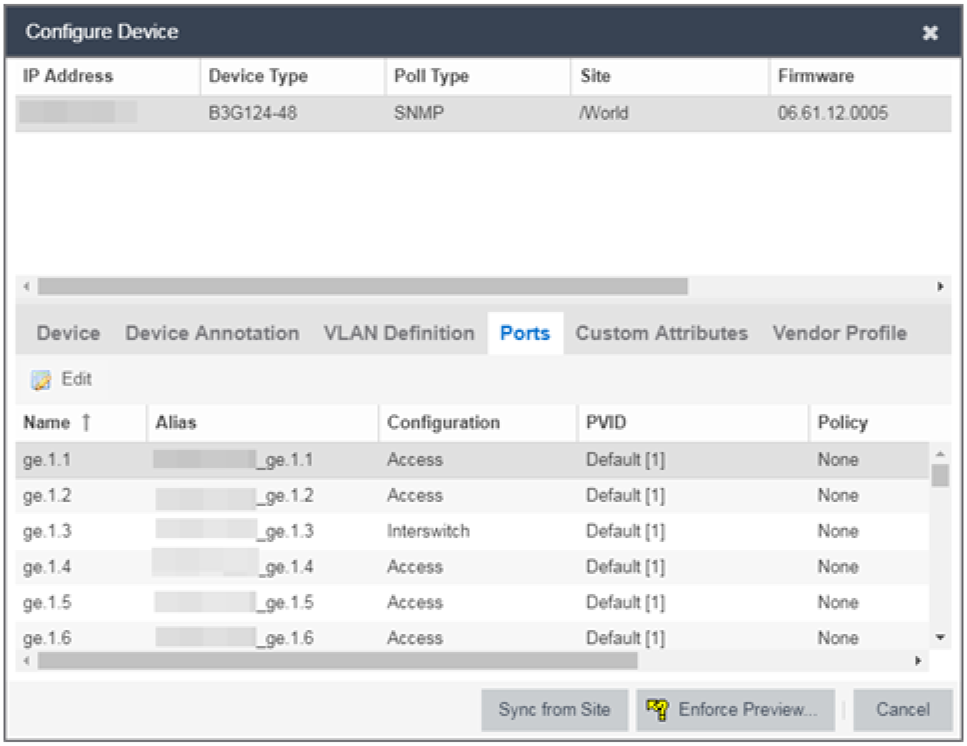
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.

3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.
5. Select the **Ports** tab.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name ↑	Alias	Configuration	PVID	Policy
ge.1.1	[redacted]_ge.1.1	Access	Default [1]	None
ge.1.2	[redacted]_ge.1.2	Access	Default [1]	None
ge.1.3	[redacted]_ge.1.3	Interswitch	Default [1]	None
ge.1.4	[redacted]_ge.1.4	Access	Default [1]	None
ge.1.5	[redacted]_ge.1.5	Access	Default [1]	None
ge.1.6	[redacted]_ge.1.6	Access	Default [1]	None

6. Select the Port on which you are configuring the VLAN.
7. Select **Edit**.
   The Port is now configurable.
8. Change the **PVID**, **Tagged**, and **Untagged** options to configure the VLAN onto the port.
9. Click **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

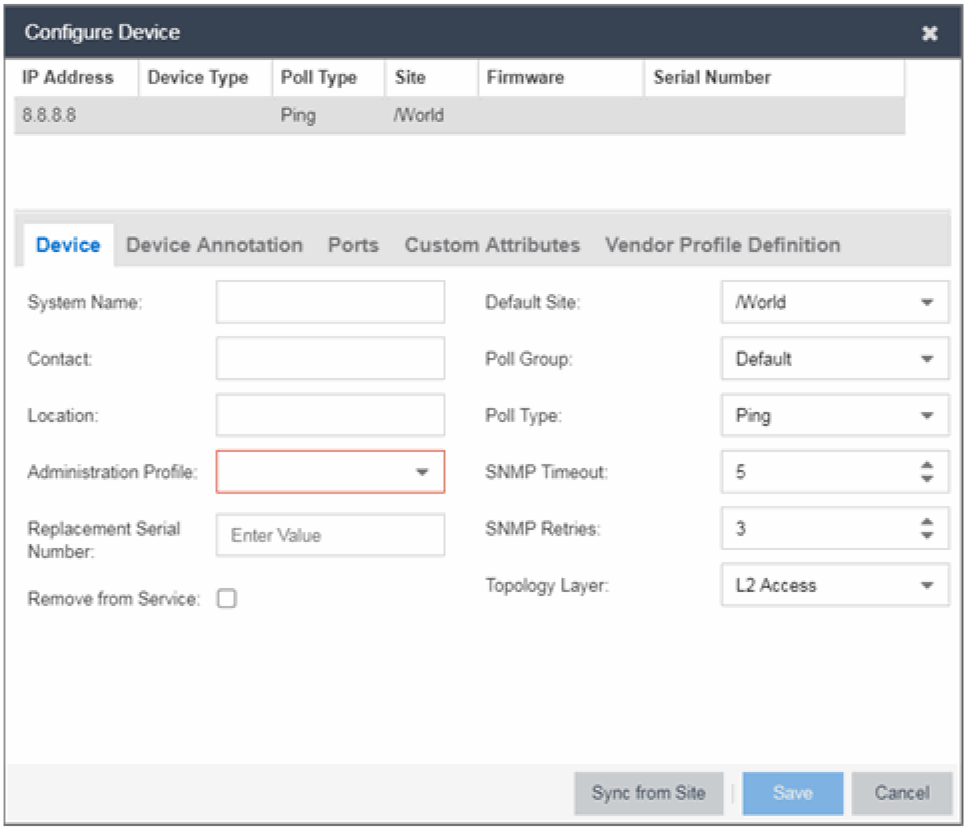
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now configured to the Ports.

To edit the name of a VLAN:

1. Launch Extreme Management Center.
2. Open the **Network** > **Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device** > **Configure Device**.
   The Configure Device window opens.

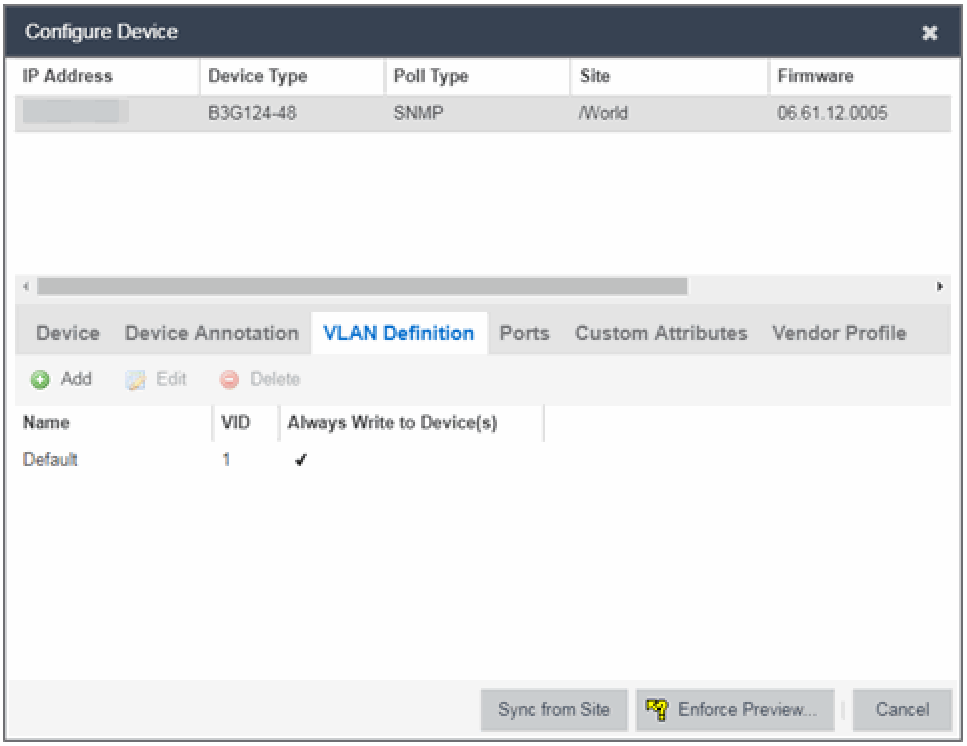


Configure Device

IP Address	Device Type	Poll Type	Site	Firmware	Serial Number
8.8.8.8		Ping	/World		

System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	□	Topology Layer:	L2 Access

5. Click the **VLAN Definition** tab.



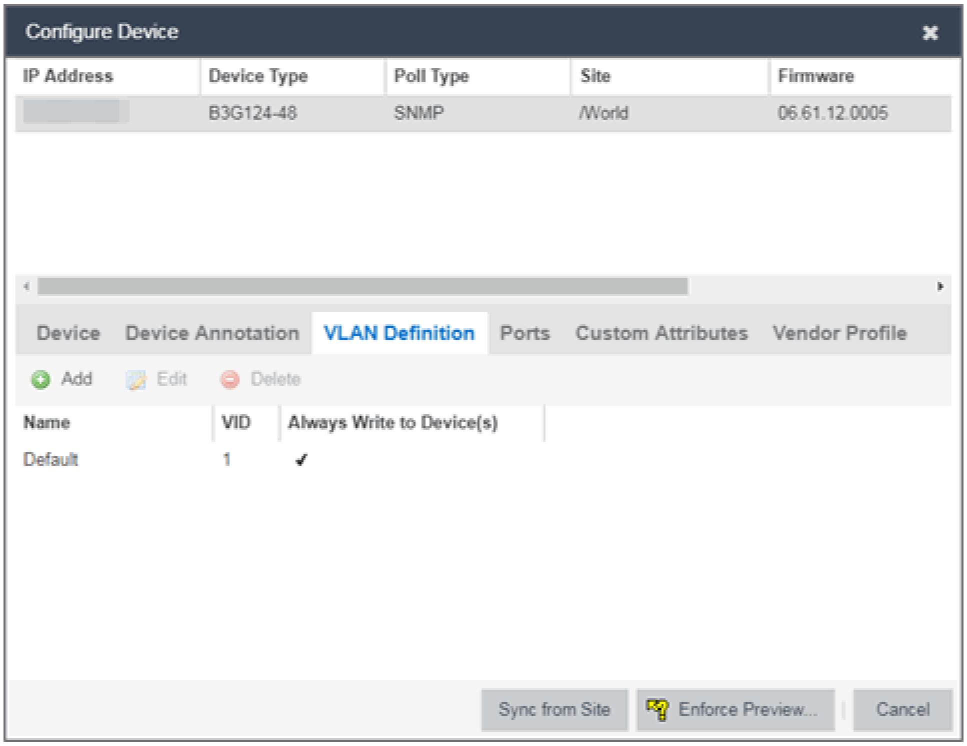
IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Click **Update**.
   The Edit pane closes.
9. Click **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.
4. Click the **VLAN Definition** tab.
   The VLAN Definition pane opens.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

5. Select the VLAN and click **Delete**.

Related Information

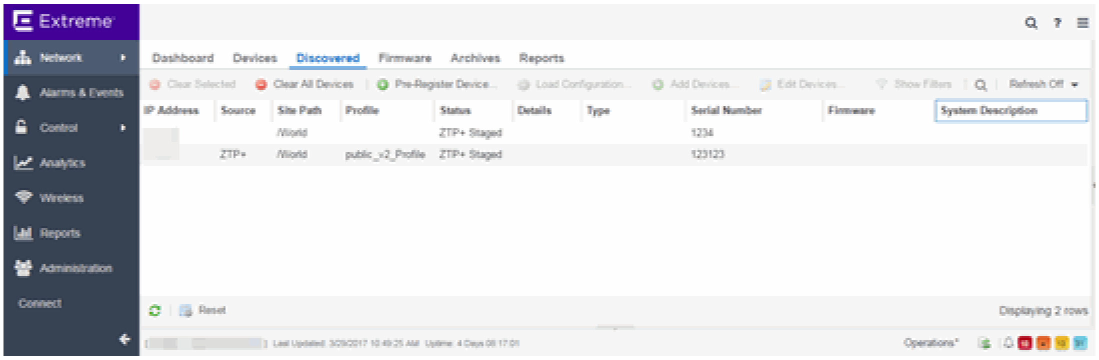
For information on related topics:

- Maps
- Devices tab

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.



IP Address	Source	Site Path	Profile	Status	Details	Type	Serial Number	Firmware	System Description
		/World		ZTP+ Staged			1234		
	ZTP+	/World	public_v2_Profile	ZTP+ Staged			123123		

Last Updated: 3/29/2017 10:49:25 AM Uptime: 4 Days 08:17:01

Devices appear on the **Discovered** tab when they are:

- Added via the Site tab without the **Automatically Add Devices** checkbox selected in the Discovered Device Actions section of the tab.
- Added using the Pre-Register Device window for your ZTP+ (Zero Touch Provisioning Plus) enabled ExtremeXOS devices.

  > **NOTE:** ZTP+ functionality requires an ExtremeXOS device on which version 21.1 is installed.

- Added using a trap to discover a ZTP (Zero Touch Provisioning) enabled device.

  > **NOTE:** ZTP functionality is not identical to ZTP+ functionality.

For instructions about how to discover devices and add them to the Extreme Management Center database, see How to Discover Devices in Extreme Management Center.

Columns

The columns on the **Discovered** tab display the details about the devices available to be added to the Extreme Management Center database.

IP Address

The **IP Address** column displays the IP address assigned to the discovered device.

Source

The **Source** column displays the IP address of the device that discovered the device and added it to the **Discovered** tab in Extreme Management Center.

Site Path

The **Site Path** column shows the site to which the device is assigned. To change the site, click the **Add Devices** button for devices with a Status of **New** or the **Edit**

Devices button for devices with a Status of **Exists** and use the **Default Site** drop-down menu in the Device section of the window to select an existing site.

You can create new sites on the **Network** > **Devices** tab.

Profile

The **Profile** column displays the profile the device is using as its administrative SNMP and CLI credentials. To change the profile, click the **Add Devices** button for devices with a Status of **New** or the **Edit Devices** button for devices with a Status of **Exists** and use the **Admin Profile** drop-down menu in the Device section of the window to select an existing profile.

You can create new profiles on the **Administration** > **Profiles** tab.

Status

The **Status** column indicates whether the device exists in the Extreme Management Center database:

- **New** — The device is discovered by Extreme Management Center, but it has not yet been added to the Extreme Management Center database.
- **Exists** — The device already exists in the Extreme Management Center database and you can monitor the device using Extreme Management Center.

Details

The **Details** column shows whether the profile is acceptable for the device as configured on the **Site** tab in the **Profiles** list. If the Reject checkbox is selected for the profile on the **Site** tab, the column displays **Reject Profile** and another profile must be selected before the device can be added to Extreme Management Center.

Type

The **Type** column displays the device type.

Serial Number

The **Serial Number** column displays the serial number of the device.

Firmware

The **Firmware** column shows the version number of the firmware or boot PROM image.

System Description

The System Description provides a complete description of the device.

Toolbar Buttons

The toolbar at the top of the tab allows you to perform various tasks on the devices on the **Discovered** tab.

Load Configuration

Click to open the Load a configuration on a Discovered Device window, which allows you to use a saved configuration for an existing device on a ZTP (zero touch provisioning) enabled device.

Clear Selected

Click to remove the currently selected device from the **Discovered** tab.

Clear All Devices

Click to remove all devices listed on the **Discovered** tab.

Pre-Register Device

Click to open the Pre-Register Device window, where you can configure a ZTP+ (zero touch provisioning plus) enabled ExtremeXOS device.

Add Devices

Opens the Add Selected Devices window, where you can configure newly discovered devices and add them to the Extreme Management Center database.

Configure Devices

Opens the Configure Device window, where you can edit an existing device's configuration.

Related Information

For information on related windows:

- Network Tab
- Devices Tab

For information on related tasks:

- How to Discover Devices in Extreme Management Center
- How to Upgrade Firmware

Load Configuration on a Discovered Device

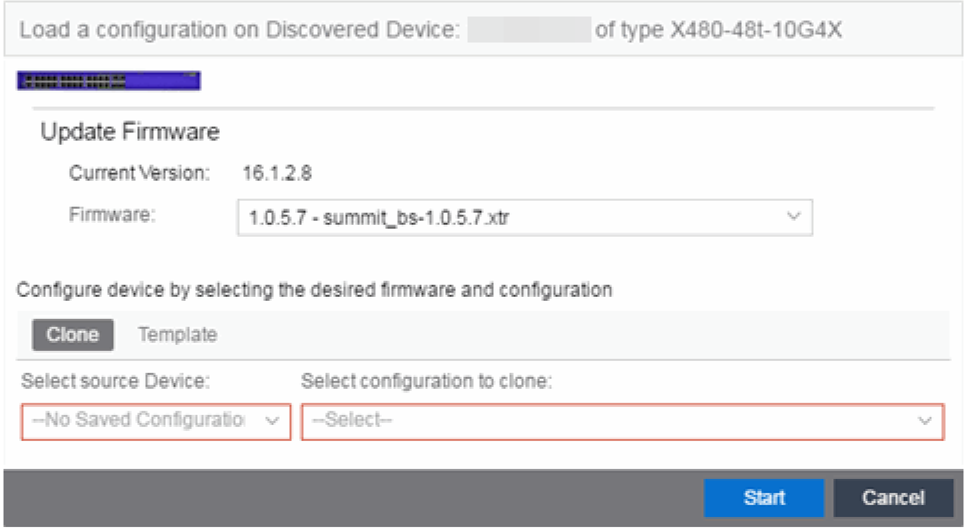
Use this window to use a saved device configuration on a device you are adding to Extreme Management Center. Devices to which you load a saved configuration must have ZTP (Zero Touch Provisioning) enabled.

This window is accessible by clicking the **Load Configuration** button or by right-clicking an existing device and selecting **Load Configuration** on the **Network** > **Discovered** tab.

The window contains two tabs, depending on the type of configuration you are loading on the new device:

- **Clone** — A configuration currently used on an existing device copied to the new device.
- **Template** — A configuration saved to Extreme Management Center as a template.

Clone



Load a configuration on Discovered Device: [redacted] of type X480-48t-10G4X

Update Firmware

Current Version: 16.1.2.8

Firmware: 1.0.5.7 - summit_bs-1.0.5.7.xtr

Configure device by selecting the desired firmware and configuration

Select source Device: --No Saved Configuratio

Select configuration to clone: --Select--

Current Version

Displays the current version of firmware installed on the device.

Firmware

Use the drop-down menu to select a new firmware version to install on the device.

Select source Device

Use the drop-down menu to select a device currently added to Extreme Management Center from which to copy the device configuration.

Select configuration to clone

Use the drop-down menu to select the configuration on the device listed in the Select source Device drop-down menu that is being cloned to the new device.

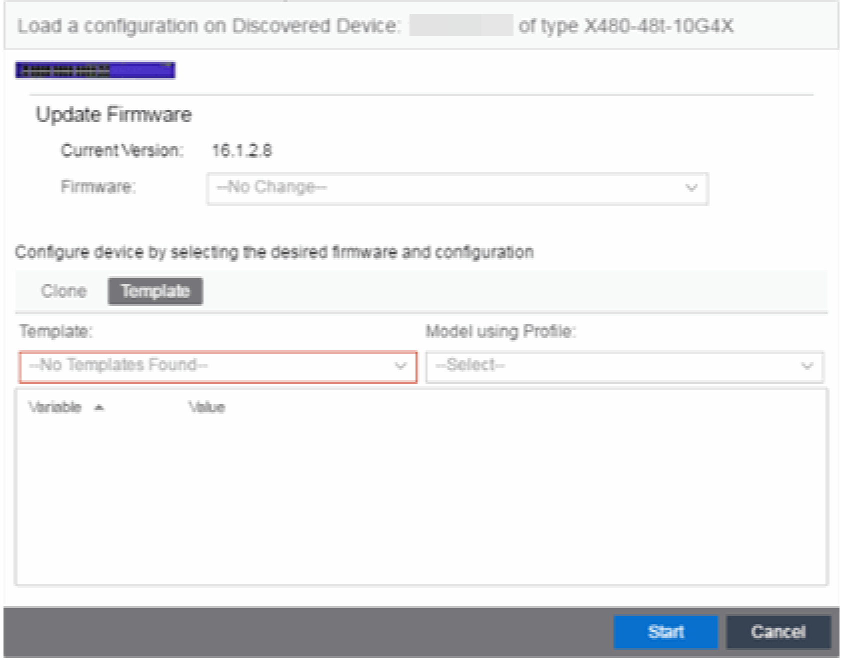
Start

Click the Start button to copy the configuration from the selected device to the new device.

Cancel

Click the Cancel button to close the window without copying the configuration.

Template



Load a configuration on Discovered Device: [redacted] of type X480-48t-10G4X

Update Firmware

Current Version: 16.1.2.8

Firmware: --No Change--

Configure device by selecting the desired firmware and configuration

Template: --No Templates Found--

Model using Profile: --Select--

Current Version

Displays the current version of firmware installed on the device.

Firmware

Use the drop-down menu to select a new firmware version to install on the device.

Template

Use the drop-down menu to select a device configuration template saved to Extreme Management Center.

Model using Profile

Use the drop-down menu to select the profile to use when modeling the template on the new device.

Start

Click the **Start** button to copy the configuration from the selected device to the new device.

Cancel

Click the **Cancel** button to close the window without copying the configuration.

Related Information

For information on related windows:

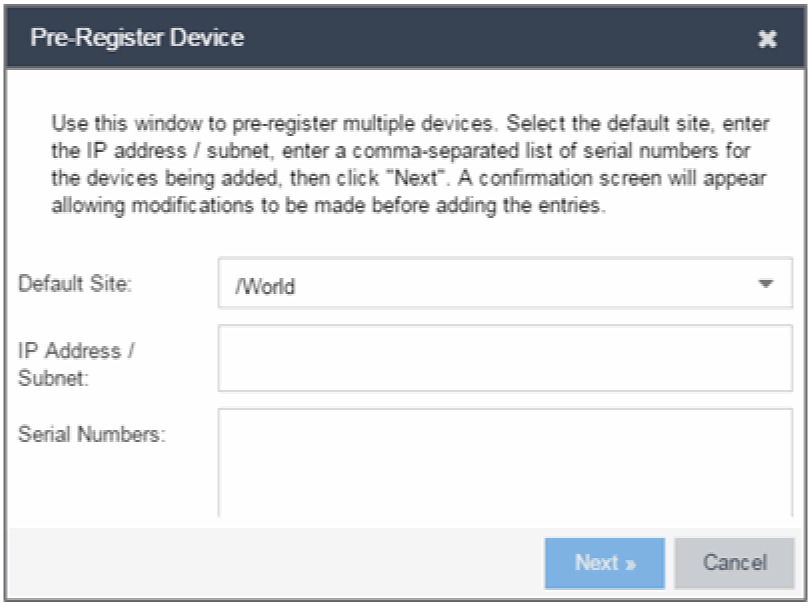
- Discovered

Pre-Register Device

Use this window to add multiple ZTP+ enabled devices to Extreme Management Center.

This window is also accessible on the **Network** > **Discovered** tab by clicking the **Pre-Register Device** button or by right-clicking an existing device and selecting **Pre-Register Device**.

Pre-Register Device Window



Use this window to pre-register multiple devices. Select the default site, enter the IP address / subnet, enter a comma-separated list of serial numbers for the devices being added, then click "Next". A confirmation screen will appear allowing modifications to be made before adding the entries.

Default Site: /World

IP Address / Subnet:

Serial Numbers:

Default Site

The site to which the devices are added.

IP Address/Subnet

Enter the device's IP address and subnet in this field. The subnet can be separated from the IP address by a slash (/) or period (.). This field is required.

Serial Number

Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas.

Next

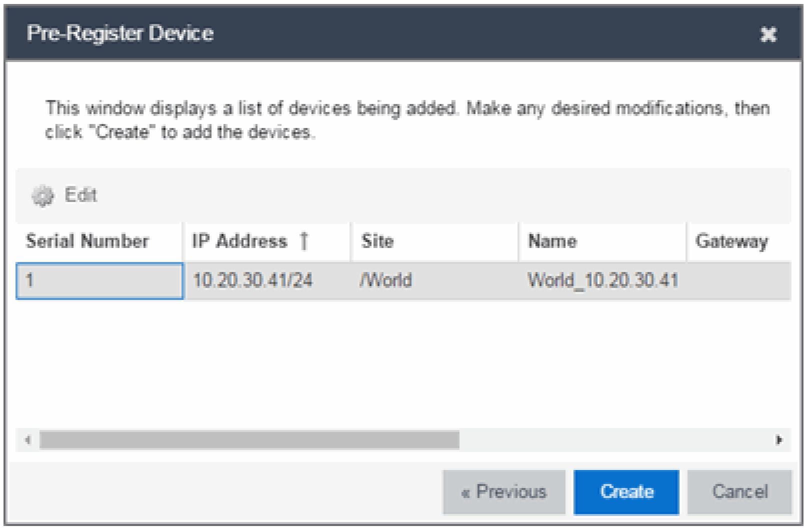
Click the **Next** button to open a confirmation window allowing you to verify the device information entered.

Cancel

Click the **Cancel** button to close the window with no changes saved.

Pre-Register Device Confirmation Window

Use this window to confirm device information before adding devices to Extreme Management Center.



This window displays a list of devices being added. Make any desired modifications, then click "Create" to add the devices.

Serial Number	IP Address ↑	Site	Name	Gateway
1	10.20.30.41/24	/World	World_10.20.30.41	

Configure

Select a device and click the **Configure** button to change the information for that device.

> **NOTE:** The **Site** can not be changed from this window.

Serial Number

The serial number of the device.

IP Address

The device's IP address.

Site

The site to which the device is added. To change the **Site**, use the Configure Device window.

Name

The name assigned to the device. The default **Name** lists includes the **Site** to which the device is assigned followed by the device's IP address.

Gateway

Enter the IP address of the switch's Access Control Gateway, if necessary.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the devices being discovered, if necessary.

DNS Server

Enter a DNS server address for the devices being discovered, if necessary.

NTP Server

Enter the NTP server address for the devices being discovered, if necessary.

Create

Click the **Create** button to add the devices listed to the Extreme Management Center database.

Related Information

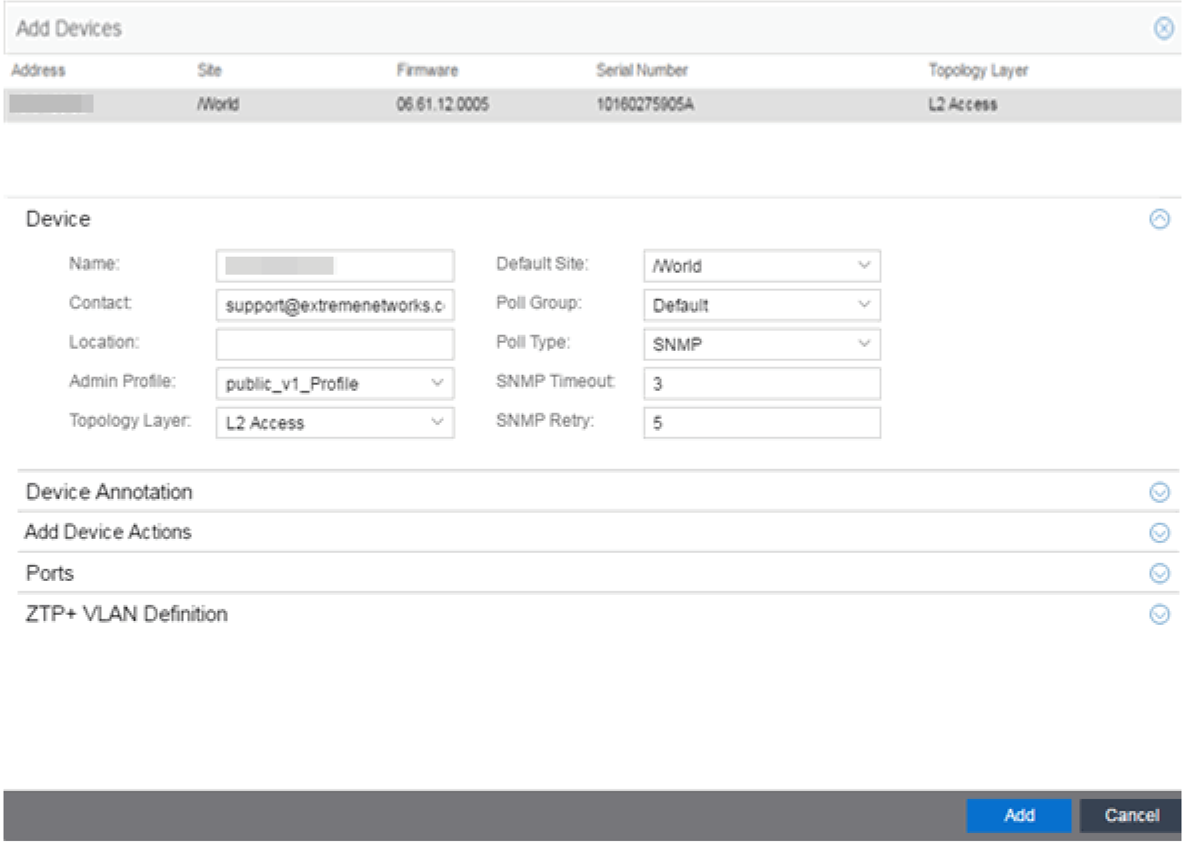
For information on related windows:

- Discovered

Add Devices

Use this window to configure a newly discovered device before you add it to the Extreme Management Center database. From this window you can configure basic information about the device, the device annotation, configure actions for the device, and add or remove ports for the device.

This window is accessible by clicking the **Add Devices** button or by right-clicking an existing device and selecting **Add Devices** on the **Network** > Discovered tab.



Address	Site	Firmware	Serial Number	Topology Layer
[redacted]	/World	06.61.12.0005	10160275905A	L2 Access

Name:	[redacted]	Default Site:	/World
Contact:	support@extremenetworks.c	Poll Group:	Default
Location:		Poll Type:	SNMP
Admin Profile:	public_v1_Profile	SNMP Timeout:	3
Topology Layer:	L2 Access	SNMP Retry:	5

If you selected multiple devices to add, they are listed at the top of the window by IP address.

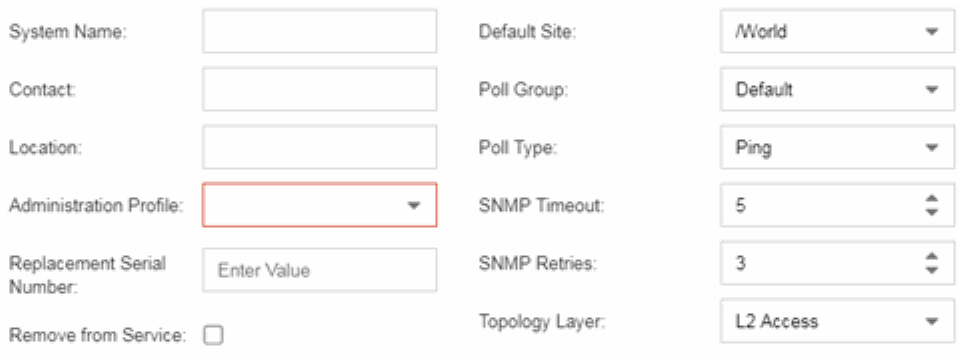
When you first open the window, only the Device section is expanded. Click a section heading to expand that section.

The Add Device window contains the following sections:

- Device
- Device Annotation
- Add Device Actions
- Ports
- ZTP+ VLAN Definition

Device

The Device section displays basic information about the device.



System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	□	Topology Layer:	L2 Access

Name

The name by which the device is known.

Contact

Allows you to specify contact information for the person maintaining the device.

Location

The physical location of the device.

Admin Profile

Use the drop-down menu to select the access Profile that gives the Discover tool administrative access to the devices you wish to discover. To create or edit a profile, open the Administration > Profiles tab.

Topology Layer

The layer and networking attributes for the device.

Default Site

Use the drop-down menu to select the map to which the device is associated.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center provides three distinct poll groups (defined in the Options > Status Polling tab) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: If Poll Type is Not Polled is specified, the Poll Group is only used if/when the Poll Type is changed to SNMP or Ping.

Poll Type

Use the drop-down menu to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping.

NOTE: On a Windows platform, device operational status cannot be determined for devices with their Poll Type set to Ping unless you are logged on and running Extreme Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time (in seconds) that Extreme Management Center waits before re-trying to contact the device. The value for this setting must be between 3 and 60 seconds.

The value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

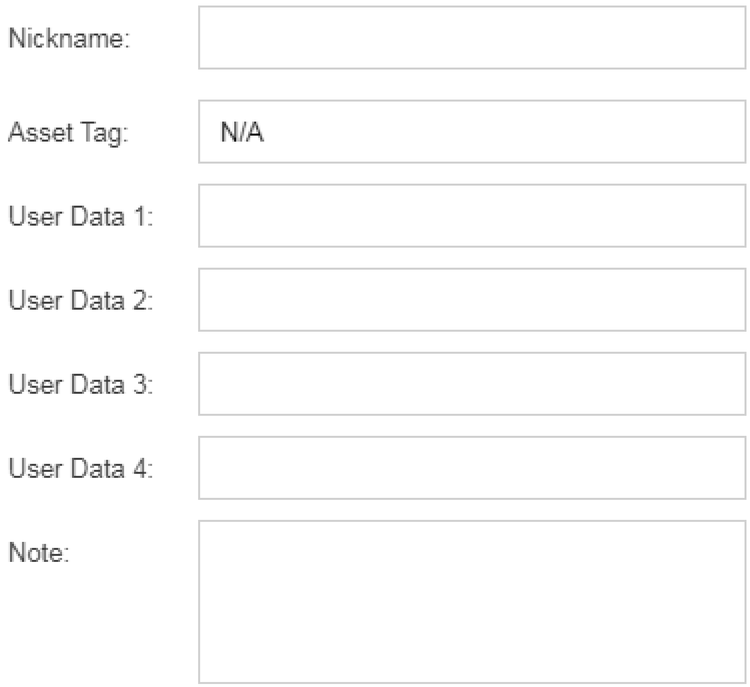
SNMP Retry

The number of attempts Extreme Management Center makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

The value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

Device Annotation

The Device Annotation section allows you to add user-defined information about the device.



Nickname:	
Asset Tag:	N/A
User Data 1:	
User Data 2:	
User Data 3:	
User Data 4:	
Note:	

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

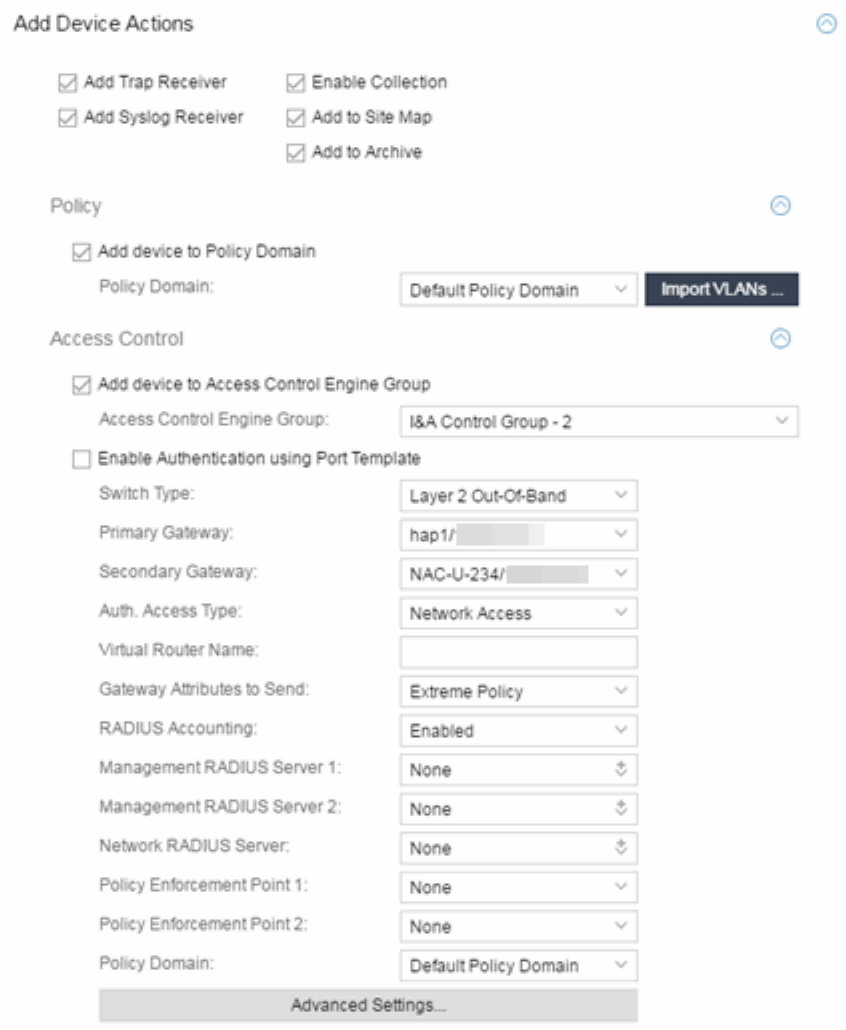
The user-defined information displayed in the devices table in the **User Data** columns.

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 Device Actions

☑ Add Trap Receiver ☑ Enable Collection
☑ Add Syslog Receiver ☑ Add to Site Map
☑ Add to Archive

Policy

☑ Add device to Policy Domain

Policy Domain: Default Policy Domain

Access Control

☑ Add device to Access Control Engine Group

Access Control Engine Group: I&A Control Group - 2

□ Enable Authentication using Port Template

Switch Type: Layer 2 Out-Of-Band
Primary Gateway: hap1/[redacted]
Secondary Gateway: NAC-U-234/[redacted]
Auth. Access Type: Network Access
Virtual Router Name:
Gateway Attributes to Send: Extreme Policy
RADIUS Accounting: Enabled
Management RADIUS Server 1: None
Management RADIUS Server 2: None
Network RADIUS Server: None
Policy Enforcement Point 1: None
Policy Enforcement Point 2: None
Policy Domain: Default Policy Domain

Add Trap Receiver

Select this checkbox if you want the devices being discovered to receive trap information it sends to Extreme Management Center.

Add Syslog Receiver

Select this checkbox to configure the devices being discovered to receive information it sends to the syslog.

Enable Collection

Select this checkbox to collect device statistics on the device being discovered you can use in Extreme Management Center reports.

Add to Site Map

Select this checkbox to add the devices being discovered to the map associated with the currently accessed site.

Add to Archive

Select this checkbox to create an archive, which saves the configurations of the devices being discovered in the Network > Archives tab.

Policy

Add device to Policy Domain

Select this checkbox to add the device to a policy domain you create on the Policy tab. Once the checkbox is selected, use the Policy Domain drop-down menu to select the policy domain to which the device is added.

Click the Import VLANs button to import the VLAN definitions from the policy selected in the Policy Domain drop-down menu.

Extreme Access Control

Add device to Extreme Access ControlEngine Group

Select this checkbox to add the device to an Extreme Access ControlEngine Group you create on the Access Control tab. Once the checkbox is selected, use the Access Control Engine Group drop-down menu to select the engine group to which the device is added.

Enable Authentication using Port Template

Select this checkbox to allow users to authenticate using a port template, configured on the Site tab.

Switch Type

Use the drop-down menu to select the type of switch you are adding:

- Layer 2 Out-Of-Band — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Extreme Access Control gateway.
- Layer 2 Out-Of-Band Data Center — A switch within a data center where virtualization and mobility are a factor. If an end-system changes location but does not move to a different Extreme Access Control engine, Extreme Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in Extreme Management Center, because only one authenticated session is allowed per end-system in Extreme Management Center.
- Layer 2 RADIUS Only — In this mode, Extreme Management Center does not require any information from the switch other than the end-system MAC

address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the Advanced Switch Settings window. IP resolution and reauthentication may not work in this mode.

- VPN - A VPN concentrator being used in an Extreme Access Control VPN deployment. In this case, you should specify one or more Policy Enforcement Points below. If you do not specify a Policy Enforcement Point, then Extreme Management Center is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down menu to select the primary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays **Determined by Load Balancer**.

Secondary Gateway

Use the drop-down menu to select the secondary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays **Determined by Load Balancer**.

NOTE: To configure additional redundant Extreme Access Control Gateways per switch (up to four), use the Display Counts option in the Display Options panel (Administration > Options > Extreme Access Control).

Auth. Access Type

Use the drop-down menu to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: For ExtremeXOS devices only. Extreme Access Control uses CLI access to perform configuration operations on ExtremeXOS devices.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. Make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Extreme Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that Extreme Management Center authenticates management login attempts against.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- Any Access - the switch can authenticate users originating from any access type.
- Management Access - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network Access - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Management Center learns about these session via RADIUS accounting. This allows Extreme Management Center to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Extreme Access Control authentication type precedence from highest to

lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- Manual RADIUS Configuration - Extreme Management Center does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using the **Policy** tab or CLI.

Virtual Router Name

Enter the name of the Virtual Router. The default value for this field is VR-Default.

WARNING: For ExtremeXOS devices only. If Extreme Management Center has not detected and populated this field, enter the Virtual Router Name carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

Gateway RADIUS Attributes to Send

Use the drop-down menu to select the RADIUS attributes included as part of the RADIUS response from the Extreme Access Control engine to the switch. You can also select Edit RADIUS Attribute Settings from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Controlengine, providing real-time connection status in Extreme Management Center.

Management RADIUS Server 1 and 2

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in Extreme Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Extreme Access Controlengine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Extreme

Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Extreme Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

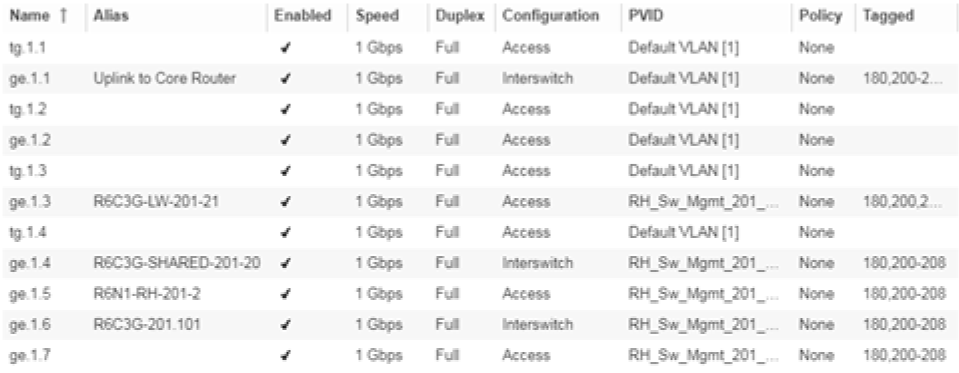
Use this option to assign the switch to a policy domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

Advanced Settings

Click the Advanced Settings button to open the Advanced Switch Settings window.

Ports

The Ports section of the Add Selected Device window allows you to enter information about the ports on a device. Click the **Add** button to add a new port to the list. Click the **Delete** button to remove a device from the list.



Name ↑	Alias	Enabled	Speed	Duplex	Configuration	PVID	Policy	Tagged
tg.1.1		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.1	Uplink to Core Router	✓	1 Gbps	Full	Interswitch	Default VLAN [1]	None	180,200-2...
tg.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
tg.1.3		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.3	R6C3G-LW-201-21	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200,2...
tg.1.4		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.4	R6C3G-SHARED-201-20	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.5	R6N1-RH-201-2	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.6	R6C3G-201.101	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.7		✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208

Name

Enter the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Configuration

Use the drop-down menu to determine the purpose of the port:

- Access — Select this option if the port connects to user end-systems.
- Interswitch — Select this option if the port is used to connect to other switches.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.

Policy

The policy assigned to the selected port.

Add

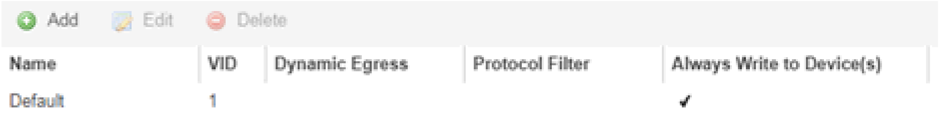
Click the Add button to add the device to the Extreme Management Center database with the current configuration.

Cancel

Click the Cancel button to close the window without adding the device to the Extreme Management Center database.

ZTP+ VLAN Definition

The ZTP+ VLAN Definition section allows you to configure VLANs on the device you are adding. To add a VLAN, click the **Add** button. You can remove a VLAN by clicking the **Delete** button.



Name	VID	Dynamic Egress	Protocol Filter	Always Write to Device(s)
Default	1			✓

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress
Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter
Indicates the VLAN uses an X-Pedition Protocol Filter.

Management
Indicates which VLAN the ExtremeXOS device uses for Management and assigns the device IP to that VLAN.

Always Write to Device(s)
Indicates if the VLAN is written to the device whether or not it is being used in a rule or role.

Related Information

For information on related windows:

- Discovered

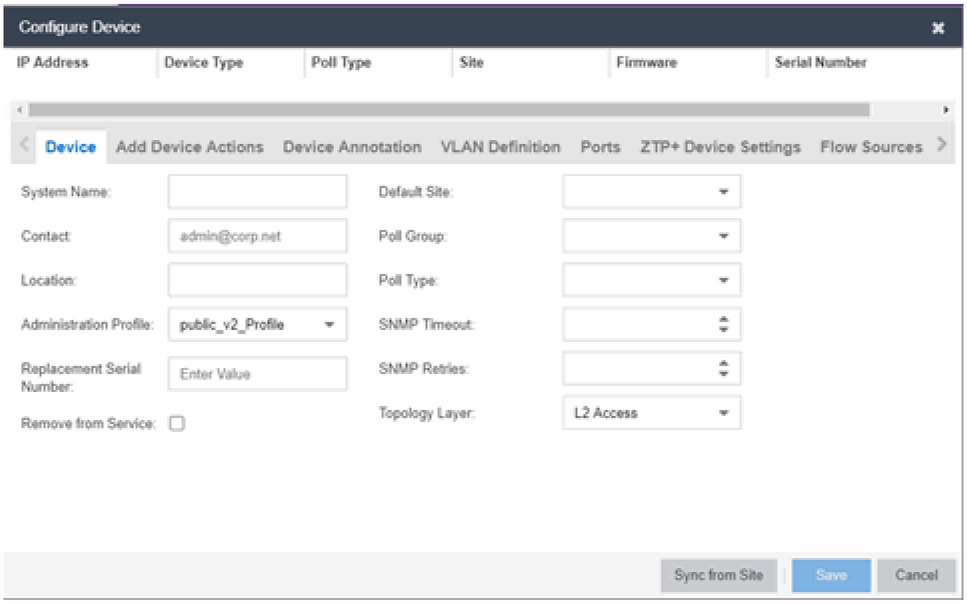
Configure Device

Use this window to configure information for an existing device. From this window you can edit basic information about the device, the device annotation, configure actions for the device, add or remove ports for the device, and configure VLANs for the device.

To access this window:

1. Open the **Network** > **Devices** tab
2. Select the **Devices** sub-tab.
3. Click the **Menu** icon (≡) or right-click on a device.
4. Select **Device** > **Configure Device**.

This window is also accessible by clicking the **Configure Device** button on the Discovered and Site tabs.



System Name:

Contact: admin@corp.net

Location:

Administration Profile: public_v2_Profile

Replacement Serial Number: Enter Value

Remove from Service: □

Default Site:

Poll Group:

Poll Type:

SNMP Timeout:

SNMP Retries:

Topology Layer: L2 Access

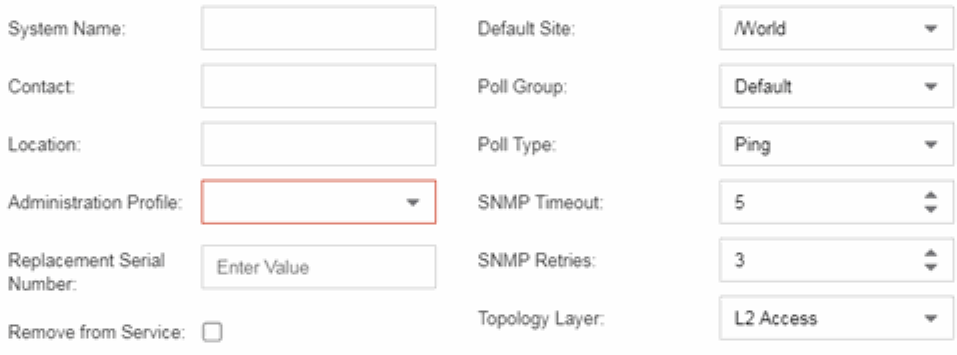
When you first open the window, the **Device** tab opens.

The **Configure Device** window contains the following tabs:

- Device
- Device Annotation
- VLAN Definition
- Ports
- ZTP+ Device Settings
- Flow Sources
- Vendor Profile
- Buttons

Device

The **Device** tab displays basic information about the device.



System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	□	Topology Layer:	L2 Access

System Name

The system name of the device. This is displayed in the **Network** > **Devices** tab tree when **Device Tree Name Format** is set to **System Name** in the Local Settings window.

Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "\" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing\John's Devices** in this field.

Location

The physical location of the device. Additionally, enter a backslash "\" between locations to create a device group in a tiered tree structure. For example, to move the device into a device group called "London" within a device group called "Europe", enter **Europe\London** in this field.

Administration Profile

Use the drop-down menu to select the access Profile that gives the Discover tool administrative access to the devices you wish to discover. To create or edit a profile, open the **Administration** > **Profiles** tab.

Replacement Serial Number

Enter the number of the device replacing this device if **Remove from Service** is selected. When entered, Extreme Management Center restores the most recent archive of the device removed from service.

Remove from Service

Select this checkbox if the device is being removed from the network. When **Remove from Service** is selected, the device is not polled and alarms are not triggered for the device.

Default Site

Use the drop-down menu to select the map to which the device is associated. For additional information, see the Maps Overview topic.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center provides three distinct poll groups (configured in the Status Polling view of the **Options** tab) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: If **Poll Type** is **Not Polled** is specified, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

Use the drop-down menu to select the Poll Type used to discover devices:

- Select **Not Polled** if you do not want to poll the devices.
- Select **Maintenance** if you do not want to poll the devices temporarily. Using this **Poll Type** allows you to search for devices set to **Maintenance** to change them back to their regular **Poll Type** once maintenance on the device is complete.
- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **Ping** for the **Poll Type** if the **Profile** for the IP Range is also set to **Ping**.

NOTE: On a Windows platform, device operational status cannot be determined for devices with their **Poll Type** set to **Ping** unless you are logged on and running Extreme Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time that Extreme Management Center waits before re-trying to contact the device. The value for this setting must be between 3 and 60 seconds.

The value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

> **NOTE:** When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

SNMP Retries

The number of attempts Extreme Management Center makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

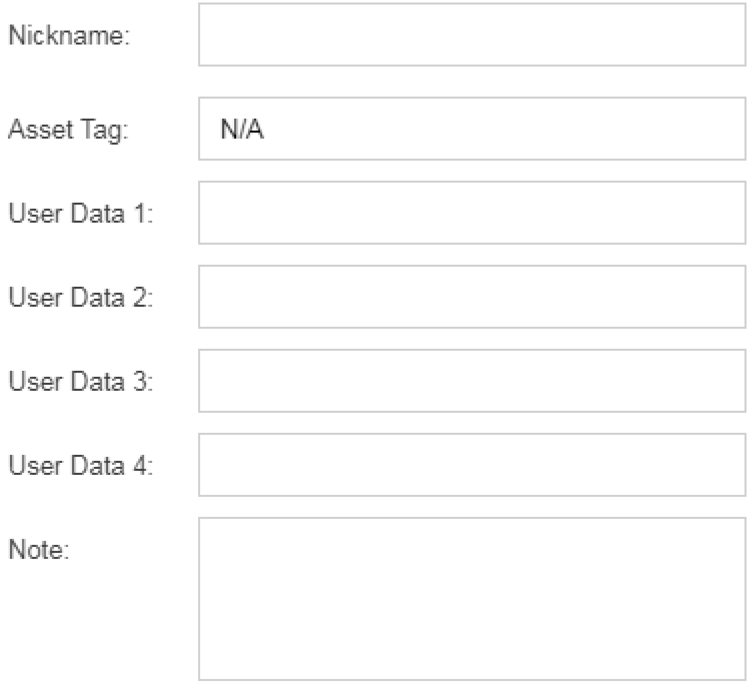
The value entered in this field overrides the default entered in the SNMP Advanced view in the Administration > Options tab.

Topology Layer

The layer and networking attributes for the device.

Device Annotation

The Device Annotation tab allows you to add user-defined information about the device.



Nickname:

Asset Tag: N/A

User Data 1:

User Data 2:

User Data 3:

User Data 4:

Note:

Nickname

The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when Nickname is selected in the

How to Display Devices in Tree menu option in the Extreme Management Center options menu in the Administration > Options tab.

Asset Tag

A unique asset number assigned to a device for inventory tracking purposes.

User Data

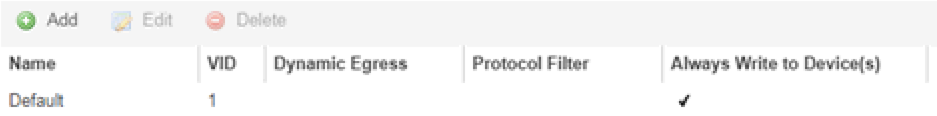
The user-defined information displayed in the devices table in the User Data columns. Additionally, enter a backslash "\" between user data to create a device group in a tiered tree structure. For example, to move the device into a device group called "Dorm 1" within a device group called "Campus", enter Campus\Dorm 1 in this field.

Notes

Additional user-defined information displayed in the devices table in the Notes column.

VLAN Definition

The VLAN Definition tab allows you to configure VLANs on the device. To add a VLAN, click the Add button. You can remove a VLAN by clicking the Delete button.



Name	VID	Dynamic Egress	Protocol Filter	Always Write to Device(s)
Default	1			✓

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress

Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter

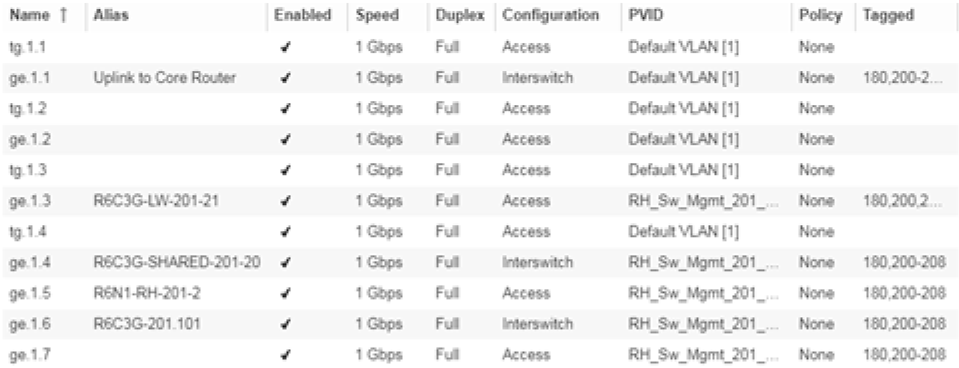
Indicates the VLAN uses an X-Pedition Protocol Filter.

Always Write to Device(s)

Indicates if the VLAN is written to the device whether or not it is being used in a rule or role.

Ports

The **Ports** tab allows you to enter information about the ports on a device. Click the **Add** button to add a new port to the list. Click the **Delete** button to remove a device from the list.



Name ↑	Alias	Enabled	Speed	Duplex	Configuration	PVID	Policy	Tagged
tg.1.1		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.1	Uplink to Core Router	✓	1 Gbps	Full	Interswitch	Default VLAN [1]	None	180,200-2...
tg.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
tg.1.3		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.3	R6C3G-LW-201-21	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200,2...
tg.1.4		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.4	R6C3G-SHARED-201-20	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.5	R6N1-RH-201-2	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.6	R6C3G-201.101	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.7		✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208

Name

Enter the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Auto Negotiation

Displays whether auto negotiation is enabled or disabled on the port. If Auto Negotiation is enabled, multi-speed selections are enabled.

Speed

Displays the current speed of the selected port. Use the drop-down list to select the speed if auto negotiation is enabled on the port.

Duplex

Displays the current duplex mode for the selected port. Use the drop-down list to select the mode if auto negotiation is enabled on the port.

Configuration

Use the drop-down menu to determine the purpose of the port:

- Access — Select this option if the port connects to user end-systems.
- Interswitch — You can also manually select this option if the port is used to connect to other switches. This option is selected by default if the port detects neighboring switches are configurable.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.
- AP — Select this option if the port is used to connect with a networking device that allows a Wi-Fi device to connect to a wired network.
- Phone — Select this option if the port is used to connect to a telephone.
- Router — Select this option if the port is used to connect to a router.
- Printer — Select this option if the port is used to connect to a printer.
- Security — Select this option if the port is used to connect to a device or devices that have been configured with security or advanced security settings.
- IoT — Select this option if the port is used to connect to an additional wireless"smart" device.
- Other — Select this option if the port is used to connect to any other device.

PVID

Select the port's VLAN ID.

LAG

Select to indicate whether the port is part of an active link aggregation group (LAG).

Authentication

Use the drop-down menu to determine whether authentication is required to access the port:

- None — No authentication is required to access the port.
- 802.1X — Select this option to require 802.1X authentication to access the port.
- MAC Auth — Select this option to require authentication based on the users MAC address.

Policy

The policy assigned to the selected port.

Tagged

Select to indicate the port's egress state is tagged.

Untagged

Select to indicate the port's egress state is untagged.

Node Alias

Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard

Select to enable Span Guard, which allows Extreme Management Center to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect

Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point ‑to ‑point interswitch links.

- If the ports receive the BPDUs, the link's State becomes Forwarding.
- If a BPDU timeout occurs on the ports, its state becomes listening until a BPDU is received.

MVRP

Indicates that the Multiple VLAN Registration Protocol (MVRP) has been enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

Update

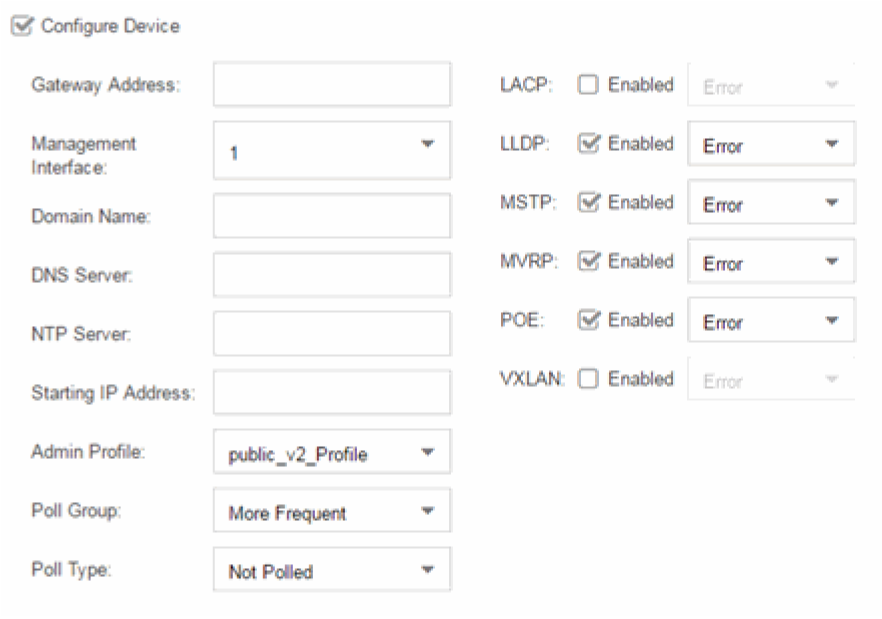
Click Update to save any changes made to the device configuration.

Cancel

Click Cancel to close the window and discard any changes.

ZTP+ Device Settings

The **ZTP+ Device Settings** tab contains basic information about the device being discovered.



☑ Configure Device

Gateway Address:		LACP:	□ Enabled	Error
Management Interface:	1	LLDP:	☑ Enabled	Error
Domain Name:		MSTP:	☑ Enabled	Error
DNS Server:		MVRP:	☑ Enabled	Error
NTP Server:		POE:	☑ Enabled	Error
Starting IP Address:		VXLAN:	□ Enabled	Error
Admin Profile:	public_v2_Profile			
Poll Group:	More Frequent			
Poll Type:	Not Polled			

Configure Device

Select this checkbox to enable ZTP+ (Zero Touch Provisioning Plus) functionality device being discovered. ZTP+ allows you to quickly add a supported device to your network with minimal configuration.

Gateway Address

Enter the **Gateway Address** for the ZTP+ devices being discovered.

Management Interface

Select the interface the ExtremeXOS device uses for Management and assigns the device IP to that interface.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices being discovered.

DNS Server

The **DNS Server** field allows you to set the DNS server address on the ZTP+ devices being discovered

NTP Server

The **NTP Server** field allows you to set the NTP server address on the ZTP+ devices being discovered.

Starting IP Address

The **Starting IP Address** field allows you to set the starting IP address of the IP address range for the ZTP+ devices being discovered.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center administrative access to the ZTP+ devices you wish to discover. Use the Profiles list in the Discover section of the **Site** tab to create or edit a profile. If you discover an existing device using a different profile than the device is already using in the database, saving the device overwrites the profile currently being used in the database.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center provides three distinct poll groups (defined in the Status Polling options (**Administration** > **Options**) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

NOTE: If you select **Not Polled**, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

Use the drop-down menu to select the **Poll Type** used to discover devices. Valid options are **SNMP**, **Ping**, and **Not Polled**. When **SNMP** is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the **Profile** specified for the IP range. If the **Profile** is set to **Ping Only**, the **Poll Type** must be set to **Ping**. If you discover an existing device using a different poll type than the device is already using in the database, saving the device overwrites the **Poll Type** currently being used in the database.

NOTE: On a Windows platform, device operational status cannot be determined for devices with their Poll Type set to Ping unless you are logged on and running Console as a user with Administrative privileges.

LACP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LACP (Link Aggregation Control Protocol) information. Select the appropriate logging level from the drop-down menu.

LLDP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LLDP (Link Layer Discovery Protocol) information. Select the appropriate logging level from the drop-down menu.

MSTP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MSTP (Multiple Spanning Tree Protocol) information. Select the appropriate logging level from the drop-down menu.

MVRP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

POE

Select the checkbox to indicate the ZTP+ devices being discovered for the site are electrically powered via the Ethernet cable.

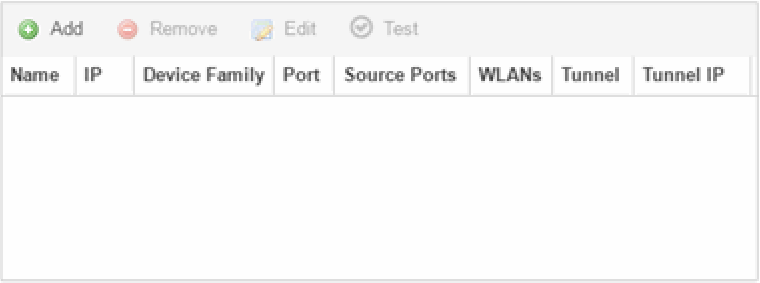
VXLAN

Select the checkbox to indicate the ZTP+ devices being discovered for this site use VXLAN to tunnel Layer 2 traffic over a Layer 3 network.

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

Flow Sources

The **Flow Sources** tab allows you to configure devices to act as flow sources for a Application Analytics engine.



Name	IP	Device Family	Port	Source Ports	WLANs	Tunnel	Tunnel IP

Name

Displays the name of the flow source device.

IP

Displays the IP address of the flow source device.

Device Family

Displays the device family of the flow source device.

Port

Indicates the mirror port attached to the Application Analytics engine or used to create the GRE tunnel.

Source Ports

Displays the ports on which flow collection is enabled.

NOTE: Policy mirrors the first 15 packets of each flow received on the Source Ports to the Application Analytics engine.

WLANs

Displays the WLANs of which the wireless controller being used as a flow source device is a member.

Tunnel

Indicates the device is configured to mirror flows using a GRE tunnel.

NOTE: If Tunnel is disabled, the Application Analytics engine must be directly attached to the flow source.

Tunnel IP

Displays the management IP address of the flow source device or the IP address of the loop-back interface on the device.

Add

Click Add to open a window from which you can select a device in Extreme Management Center to add as a flow source.

Remove

Select a flow source device in the table and click Remove to remove the device as a flow source.

Edit

Click Edit to open a window from which you can change the configuration of a flow source device.

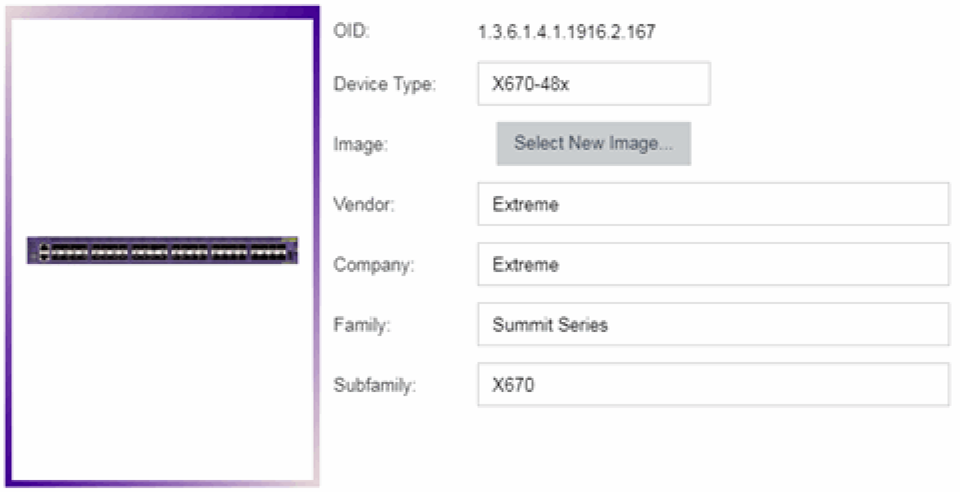
Test

Click **Test** to verify the GRE tunnel end-points can communicate.

> **NOTE:** **Test** is only available if **Tunnel** is enabled.

Vendor Profile

The **Vendor Profile** tab allows you to edit configurations for devices. The configuration you select determines the reports available for the device in its DeviceView and lets you choose the FlexView filters that apply to the device. You can also enter additional information about the device to help identify it in Extreme Management Center as well as identify the scripts that apply to the device.



OID: 1.3.6.1.4.1.1916.2.167

Device Type: X670-48x

Image:

Vendor: Extreme

Company: Extreme

Family: Summit Series

Subfamily: X670

OID

Displays the Object Identifier for the device.

Device Type

Displays the specific type of device.

> **NOTE:** When **Device Type** is blank:
>
> - The tab is named **New Vendor Profile**.
> - You cannot use special characters when creating a new **Device Type**.

Image

Indicates the image file used for the device in the DeviceView and Maps.

Vendor

Displays the vendor who sold the device.

Company

Displays the company that manufactures the device.

Family

Displays the group of devices to which the device belongs, known as the device family in Extreme Management Center.

Subfamily

Displays a smaller grouping to which the device belongs, if applicable.

Buttons

Enforce Preview

Click to open the Compare Device Configuration window, from which you can view and compare your current configuration and the proposed new configuration. This window allows you to verify all of the changes you are making to your devices and then enforce those changes to the device. This button displays after making a change that affects the device.

Sync from Site

Click to copy the default configurations for the site to all the selected devices.

Save

Click to save any changes you make to a device in Extreme Management Center.

Cancel

Click to discard any unsaved changes and close the window.

Related Information

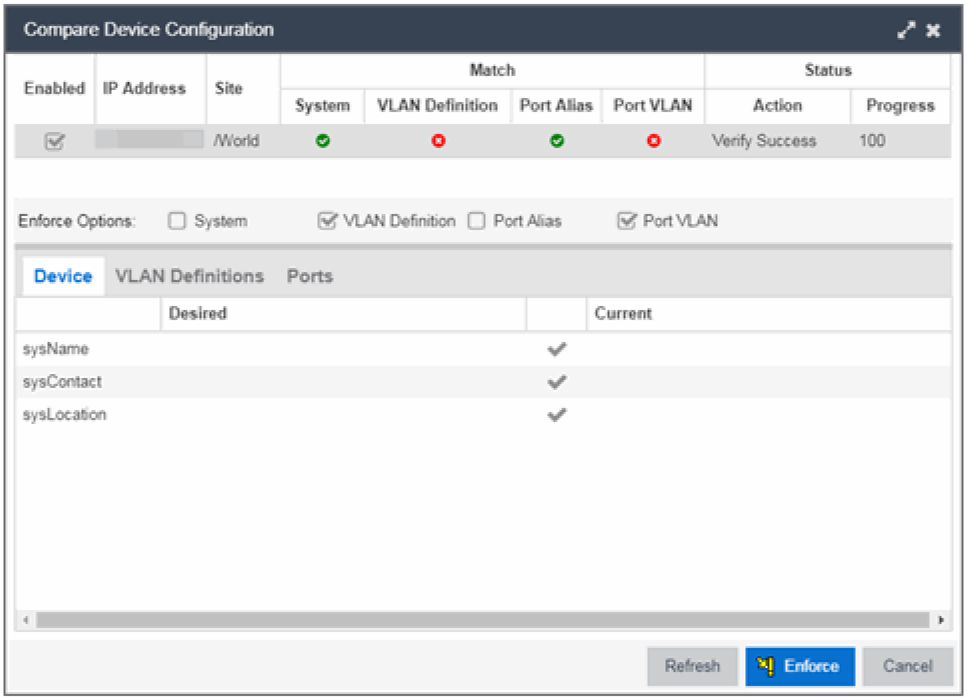
For information on related windows:

- Edit Policy Mapping Configuration Window

Compare Device Configuration

This window allows you to preview changes you make to a device configuration and then enforce them to the device.

To access this window click **Enforce Preview** in the Configure Device window.



			Match				Status	
Enabled	IP Address	Site	System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
☑	[redacted]	/World	✓	✗	✓	✗	Verify Success	100

Enforce Options: ☐ System ☑ VLAN Definition ☐ Port Alias ☑ Port VLAN

	Desired		Current
sysName		✓	
sysContact		✓	
sysLocation		✓	

The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the bottom of the window.

Devices on which the current configuration matches the desired configuration display a check icon (✓), while devices on which differences are detected display a red x (✗). The System column indicates the whether the information on the **Device** tab matches, the VLAN Definition column indicates whether the information on the **VLAN Definitions** tab matches, and the Port Alias and Port VLAN columns indicate whether the information on the **Ports** tab matches.

The Enforce Options section of the window allows you to select the changes you want to make on the device. Select **System** to push changes you make on the **Device** tab to the device, select **VLAN Definition** to push changes you make on the **VLAN Definitions** tab, select **Port Alias** to push changes you make to the top table on the Ports tab, and select **Port VLAN** to push changes you make to the Port VLAN Details table on the **Ports** tab.

NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

In each tab, the configurations are separated into two columns:

- The Desired column shows the configuration you are saving to the device on the next enforce.
- The Current column shows the configuration currently on the device.

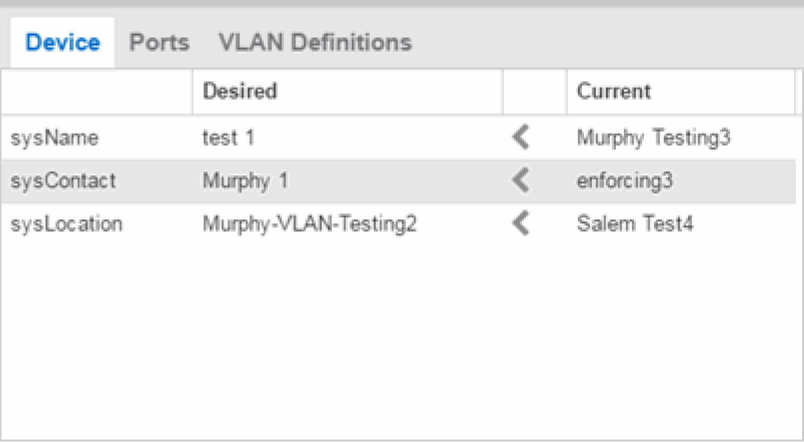
A check mark between the columns (✓) indicates the Current configuration matches the Desired configuration.

A left arrow icon (‹) indicates the configurations do not match. Clicking it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

Click **Enforce** to save your changes to the device.

Device

The **Device** tab displays any changes to basic information about the device.



	Desired		Current
sysName	test 1	<	Murphy Testing3
sysContact	Murphy 1	<	enforcing3
sysLocation	Murphy-VLAN-Testing2	<	Salem Test4

sysName

The name by which the device is known.

sysContact

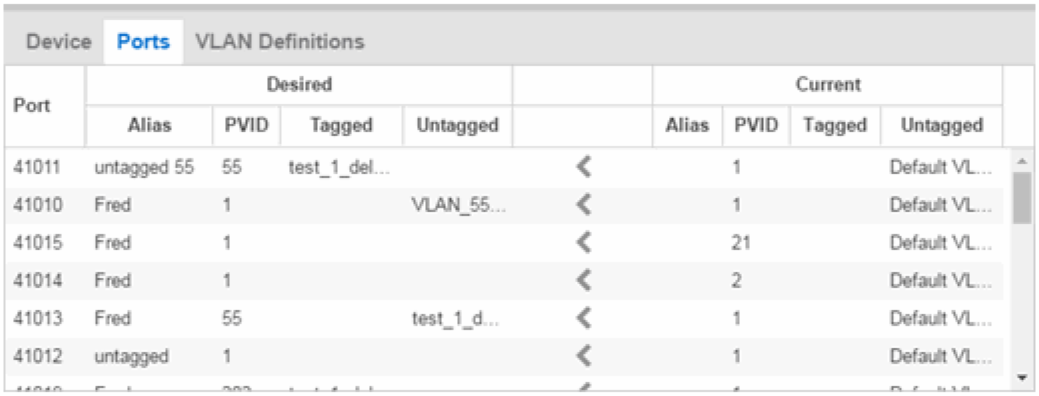
Allows you to specify contact information for the person maintaining the device.

sysLocation

The physical location of the device.

Ports

The **Ports** tab displays any changes to the configuration of ports on the device.



Port	Desired					Current			
	Alias	PVID	Tagged	Untagged		Alias	PVID	Tagged	Untagged
41011	untagged 55	55	test_1_del...		<		1		Default VL...
41010	Fred	1		VLAN_55...	<		1		Default VL...
41015	Fred	1			<		21		Default VL...
41014	Fred	1			<		2		Default VL...
41013	Fred	55		test_1_d...	<		1		Default VL...
41012	untagged	1			<		1		Default VL...

Port

The name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Shows the alias for the port, if one is assigned.

PVID

The port's VLAN assignment. Possible values are 1 through 4094.

Tagged

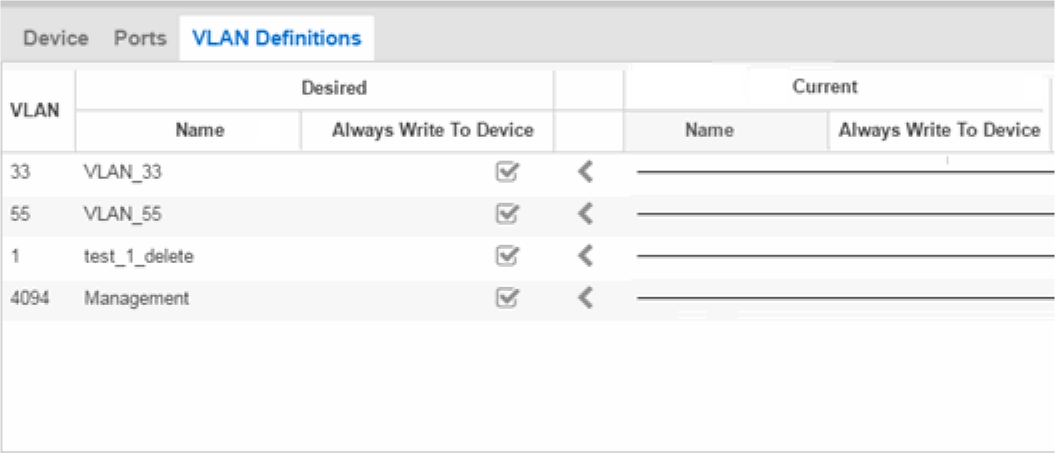
The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged

The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).

VLAN Definitions

The **VLAN Definitions** tab displays any changes to the VLANs defined for the device selected at the top of the window.



VLAN	Desired			Current	
	Name	Always Write To Device		Name	Always Write To Device
33	VLAN_33	☑	<		
55	VLAN_55	☑	<		
1	test_1_delete	☑	<		
4094	Management	☑	<		

VLAN

A unique numerical identifier of the VLAN.

Name

The name of the VLAN.

Always Write to Device(s)

Indicates whether or not the VLAN is written to the device(s) when you enforce, or compared to the actual VLANs on the device(s) when you verify.

Related Information

For information on related topics:

- VLAN Concepts
- Configure Device
- Site Tab

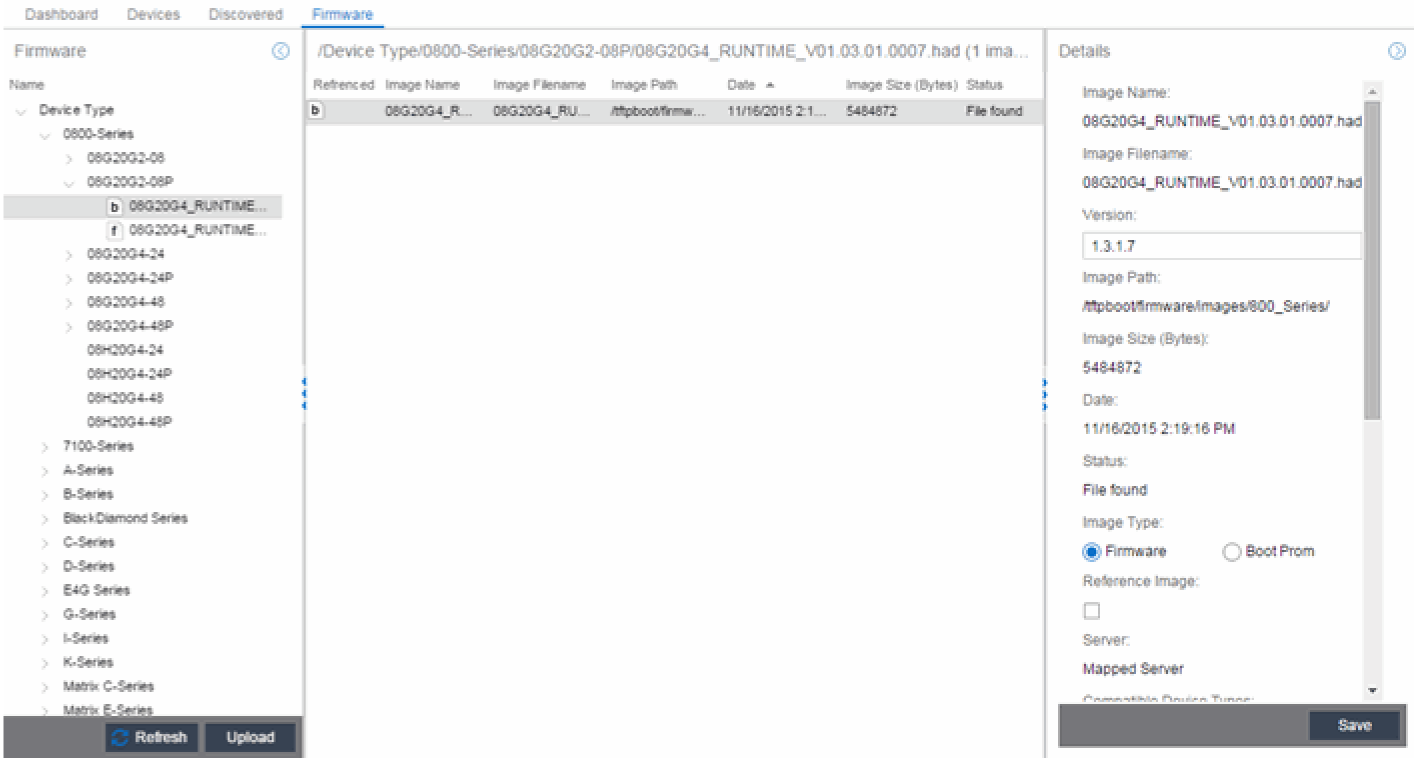
Firmware

The **Firmware** tab allows you to upload firmware and boot PROM images to Extreme Management Center and assign them to the devices on your network.

To access the **Firmware** tab, open the **Network** tab and select the **Firmware** tab.

The tab is divided into three sections:

- Firmware Tree
- Device Type Images Section
- Details Section



/Device Type/0800-Series/08G20G2-08P/08G20G4_RUNTIME_V01.03.01.0007.had (1 ima...

Refrenced	Image Name	Image Filename	Image Path	Date ▲	Image Size (Bytes)	Status
b	08G20G4_R...	08G20G4_RU...	/tftpboot/firmw...	11/16/2015 2:1...	5484872	File found

Image Name:
08G20G4_RUNTIME_V01.03.01.0007.had

Image Filename:
08G20G4_RUNTIME_V01.03.01.0007.had

Version:
1.3.1.7

Image Path:
/tftpboot/firmware/images/800_Series/

Image Size (Bytes):
5484872

Date:
11/16/2015 2:19:16 PM

Status:
File found

Image Type:
● Firmware ○ Boot Prom

Reference Image:
□

Server:
Mapped Server

Firmware Tree

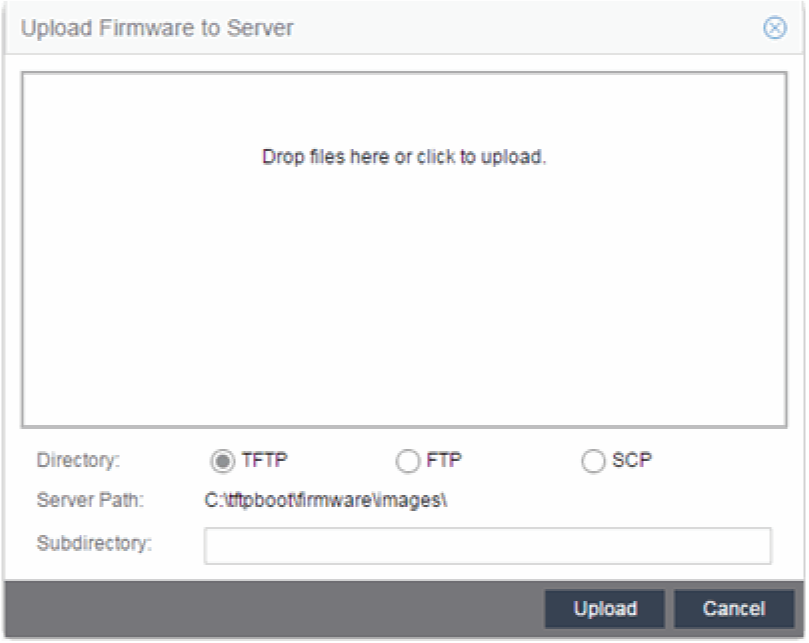
The **Firmware** tree in the left panel displays firmware and boot PROM images grouped according to product family and device type. It provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a firmware discovery or refresh. The Unknown folder contains images that Extreme Management Center could not correlate to a device type.

Name

The **Name** navigation tree lists the product families and device types to which you can assign the firmware or boot PROM image.

Upload

Click the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the Extreme Management Center server. This allows anyone with access to Extreme Management Center to download the image file to a device.


Upload Firmware to Server

Drop files here or click to upload.

Directory: ● TFTP ○ FTP ○ SCP

Server Path: C:\tftpboot\firmware\images\

Subdirectory:

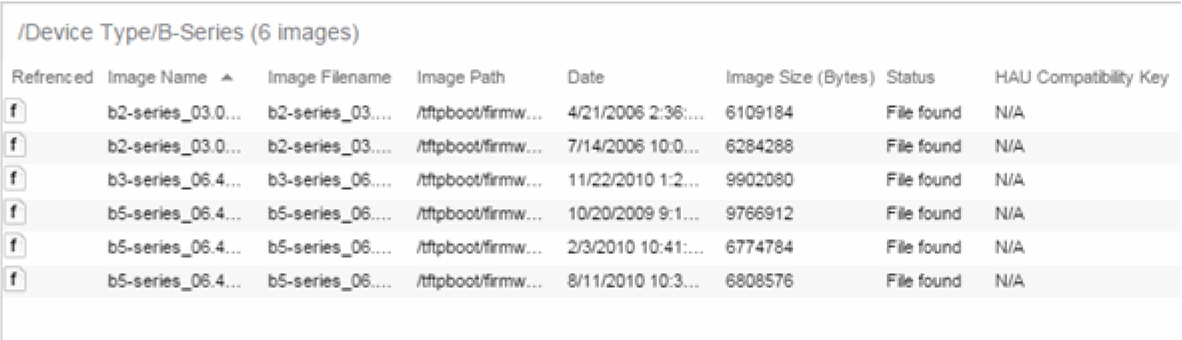
For additional information on how to upload a firmware or boot PROM image, see How to Upgrade Firmware.

Refresh

Click the **Refresh** button to synchronize the images displayed in the Firmware left-panel with the firmware and boot PROM images on the Extreme Management Center server. Clicking this button checks for any firmware and boot PROM images saved in the Firmware Directory Path (configured on the **Administration** > **Options** > Inventory Manager tab) on the Extreme Management Center server and adds or removes images from the Firmware left-panel in Extreme Management Center to match.

Device Type Images Section

The Device Type Images section displays the firmware and boot PROM images that match the device type selected in the Firmware left-panel. To save a firmware or boot PROM image to a device, select it from the list and save the image to the device in the Details section of the **Firmware** tab.



/Device Type/B-Series (6 images)

Refrenced	Image Name ▲	Image Filename	Image Path	Date	Image Size (Bytes)	Status	HAU Compatibility Key
f	b2-series_03.0...	b2-series_03....	/tftpboot/firmw...	4/21/2006 2:36:...	6109184	File found	N/A
f	b2-series_03.0...	b2-series_03....	/tftpboot/firmw...	7/14/2006 10:0...	6284288	File found	N/A
f	b3-series_06.4...	b3-series_06....	/tftpboot/firmw...	11/22/2010 1:2...	9902080	File found	N/A
f	b5-series_06.4...	b5-series_06....	/tftpboot/firmw...	10/20/2009 9:1...	9766912	File found	N/A
f	b5-series_06.4...	b5-series_06....	/tftpboot/firmw...	2/3/2010 10:41:...	6774784	File found	N/A
f	b5-series_06.4...	b5-series_06....	/tftpboot/firmw...	8/11/2010 10:3...	6808576	File found	N/A

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

This column displays the HAU Compatibility Key, if one is detected on the firmware image. The HAU Compatible column (in the Assignments table) displays whether the firmware image and the device are HAU compatible. HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, Extreme Management Center performs the upgrade using this feature, if the HAU firmware key on the current firmware and the key on the newly selected firmware are compatible.

The following table explains the upgrade procedure for HAU devices:

HAU Mode on Device	New Image HAU Compatible?	Upgrade Procedure
Never	Yes	Standard Upgrade
Never	No	Standard Upgrade
If Possible	Yes	HAU
If Possible	No	Standard Upgrade
Always	Yes	HAU
Always	No	Upgrade Fails

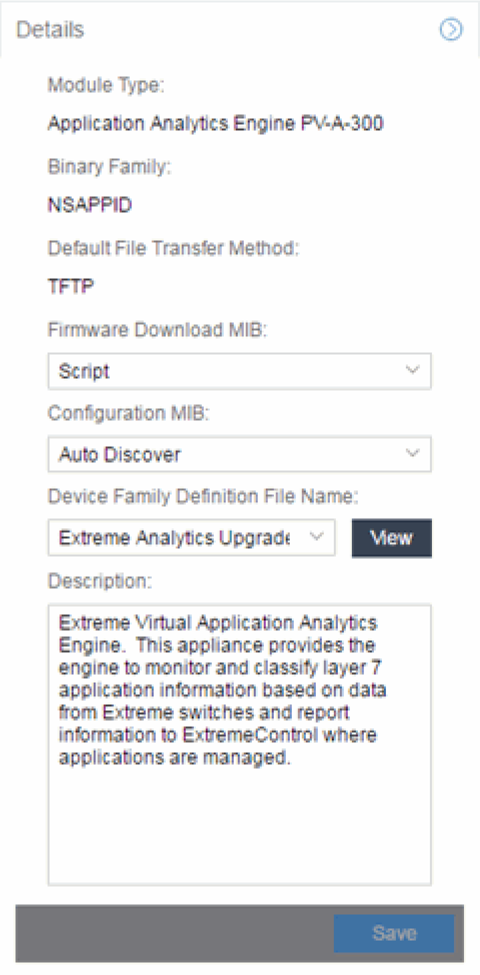
NOTE: Firmware images that were discovered with a NetSight version prior to 4.4 need to be removed from Extreme Management Center (right-click the image on the **Firmware** tab and select **Delete Image**) and then rediscovered in order to populate the compatibility key field.

Details Section

The Details right-panel displays additional information about a device type or a firmware or boot PROM image, depending on what you select in the left-panel or in the Device Type Images section of the window.

Device Type Details

Selecting a device type in the Firmware Tree left-panel opens the details for that device in the Details right-panel.



Details

Module Type:
Application Analytics Engine PV-A-300

Binary Family:
NSAPPID

Default File Transfer Method:
TFTP

Firmware Download MIB:
Script

Configuration MIB:
Auto Discover

Device Family Definition File Name:
Extreme Analytics Upgrade

Description:
Extreme Virtual Application Analytics Engine. This appliance provides the engine to monitor and classify layer 7 application information based on data from Extreme switches and report information to ExtremeControl where applications are managed.

Module Type

The device's model number or hardware type.

Binary Family

The binary family to which the device type belongs. Device types in the same binary family share the same firmware image.

Default File Transfer Method

The default file transfer method for this device type. To set the default file transfer method for a device type, right-click on a device type in the Firmware Tree left-panel and select Default File Transfer Method. You can also set the default file transfer method for groups of devices of the same series by right-clicking on the device type's parent folder and selecting Default File Transfer Method.

Firmware Download MIB

The Firmware Download MIB supported by this device type. If the device type supports more than one Firmware Download MIB, use the drop-down menu to select the desired MIB. In addition to a list of MIBs, other menu options include:

- Auto Discover — Extreme Management Center reads the Firmware Download MIB on the first device of this device type that you add or import and displays it here. Extreme Management Center then uses that MIB to perform firmware and boot PROM downloads on all devices of this device type.
- Disabled — Firmware download functionality is not allowed for this device type.
- Script — Allows the firmware download function to be executed through the use of a script. This option is used when upgrading Extreme Access Control and Application Analytics engines as well as for third-party devices that do not support the required SNMP MIBs. For information on using scripts to upgrade Extreme Access Control and Application Analytics engines, refer to How to Upgrade Firmware.

Configuration MIB

The Configuration MIB supported by this device type. If the device type supports more than one Configuration MIB, use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- Auto Discover — Extreme Management Center reads the Configuration MIB on the first device of this device type that you add or import and displays it here. Extreme Management Center then uses that MIB to perform archive operations on all devices of this device type.

- **Disabled** — Archive functionality is not allowed for this device type.
- **Script** — Allows the archive functionality to be executed through the use of a script. This option is used for third-party devices that do not support the required SNMP MIBs.

Device Family Definition File Name

Select the file containing the scripts you are using if **Script** is selected for **Firmware Download MIB** and/or **Configuration MIB**. Include all the scripts and data for each supported Extreme Management Center function for specific third-party devices in this file.

Extreme Management Center provides sample Definition Files for Extreme, Enterasys, Cisco Systems, and Hewlett Packard devices. Click the **View** button to open the Script Details window, from which you can view the script.

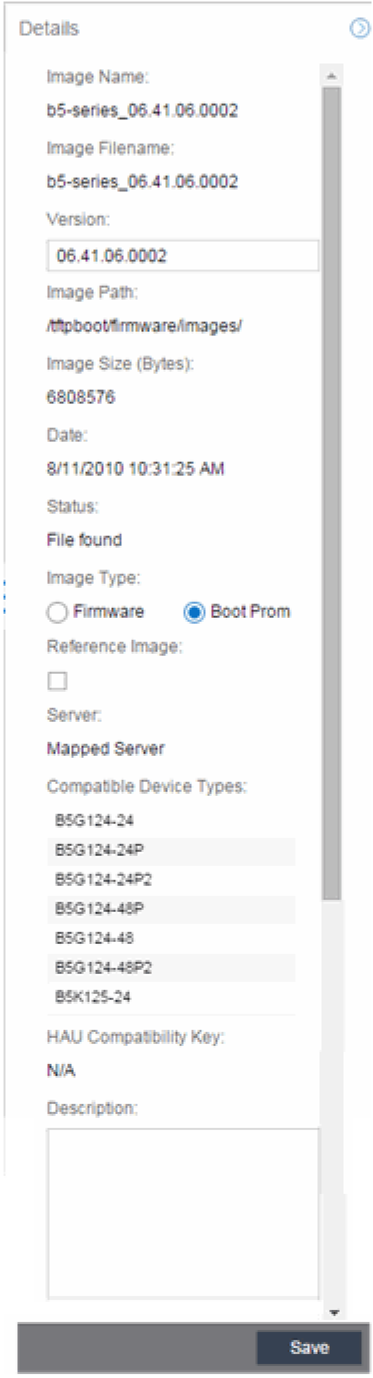
Description

Allows you to enter a description for the device.

Click **Save** to save any changes.

Firmware/boot PROM Image Details

Use this section to edit the version number of the image, the type of image (firmware or boot PROM), and enter a description for the image.



Details

Image Name:
b5-series_06.41.06.0002

Image Filename:
b5-series_06.41.06.0002

Version:
06.41.06.0002

Image Path:
/tftpboot/firmware/images/

Image Size (Bytes):
6808576

Date:
8/11/2010 10:31:25 AM

Status:
File found

Image Type:
○ Firmware ● Boot Prom

Reference Image:
□

Server:
Mapped Server

Compatible Device Types:
B5G124-24
B5G124-24P
B5G124-24P2
B5G124-48P
B5G124-48
B5G124-48P2
B5K125-24

HAU Compatibility Key:
N/A

Description:

Image Name

The name of the image as it is displayed in the left-panel Firmware tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

Image Filename

The full name of the image as it appears in your firmware images directory.

Version

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field displays N/A (not available). Enter a version number and 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, Extreme Management Center attempts to perform an HAU upgrade if the HAU firmware compatibility key is the same for the currently running firmware and the newly selected firmware.

NOTE: Firmware images discovered with a version of Extreme Management Center prior to 4.4 need to be removed and rediscovered to populate the compatibility key field.

Description

Use this field to add a brief description of the image and any information regarding its use. Click **Save** to save any changes.

Save

Saves any changes you have made to the version or description field.

Related Information

For information on related windows:

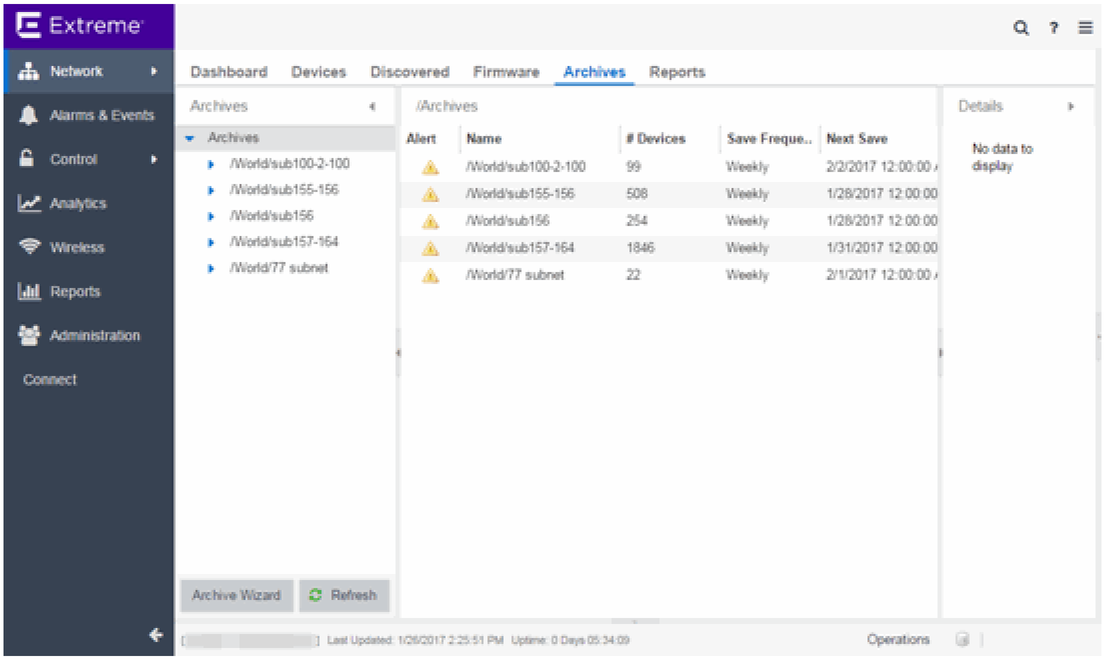
- Network
- Devices

For information on related tasks:

- How to Upgrade Firmware

Archives

The **Archives** tab allows you to create new archives (saved configurations) via the Archive Wizard, edit an archive's attributes including devices, schedule, process, and setup, and view all of the archives for a particular device family, or see specific details about an individual archive. Additionally, with a governance license, you can test your device archives for compliance with industry standards and regulations.



Alert	Name	# Devices	Save Freque...	Next Save
⚠	/World/sub100-2-100	99	Weekly	2/2/2017 12:00:00
⚠	/World/sub155-156	508	Weekly	1/28/2017 12:00:00
⚠	/World/sub156	254	Weekly	1/28/2017 12:00:00
⚠	/World/sub157-164	1846	Weekly	1/31/2017 12:00:00
⚠	/World/77 subnet	22	Weekly	2/1/2017 12:00:00

Last Updated: 1/26/2017 2:25:51 PM Uptime: 0 Days 05:34:09

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** C — 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** C▤ — 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 Archive Name Panel.
  - 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 Archive Version Panel.
  - 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 Archive File Panel.
- 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:

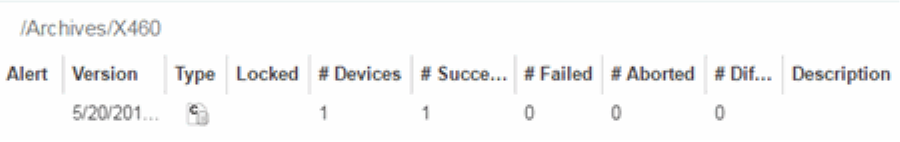
- Archive Name Panel
- Archive Version Panel
- Archive File Panel

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.



/Archives/X460

Alert	Version	Type	Locked	# Devices	# Succe...	# Failed	# Aborted	# Dif...	Description
	5/20/201...	C▤		1	1	0	0	0	

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:

- C — Device Configuration Data
- ▤ — Capacity Planning Data
- C▤ — 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

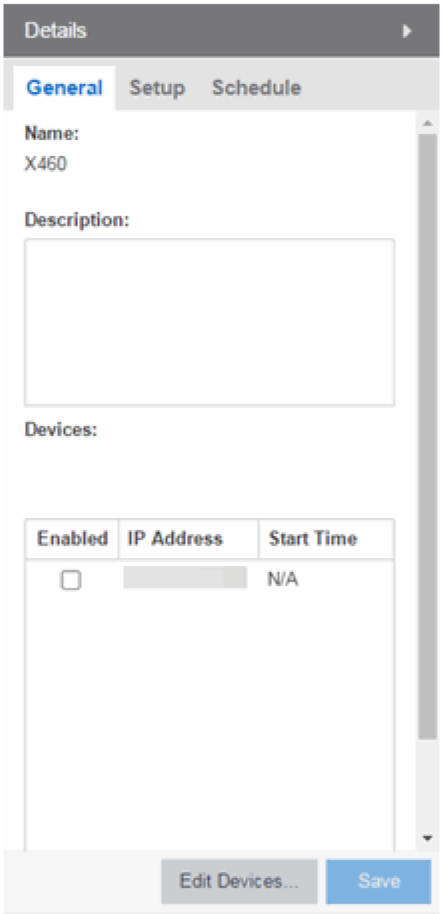
For information on related tasks:

- 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



Details

General Setup Schedule

Name:
X460

Description:

Devices:

Enabled	IP Address	Start Time
□		N/A

Name

The name of the archive operation. You cannot change the archive name here. To rename an archive, right-click the archive in the left-panel of the **Archive** tab, and then select **Rename**.

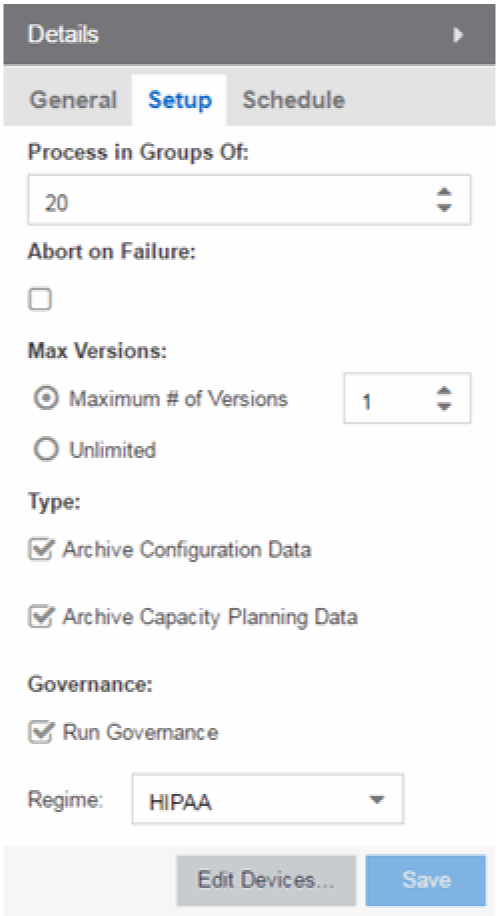
Description

A brief description to help you identify the archive operation.

Devices

Lists the devices selected for the operation. Using the **Enabled** checkboxes, select or deselect the devices you want to archive. To edit this device list, click [Edit Devices](#).

Setup



Process in Groups Of: 20

Abort on Failure: ☐

Max Versions:

● Maximum # of Versions 1

○ Unlimited

Type:

☑ Archive Configuration Data

☑ Archive Capacity Planning Data

Governance:

☑ Run Governance

Regime: HIPAA

Process in Groups Of

The archive is performed simultaneously on the number of devices specified in the **Process in Groups Of** field. Enter the value **1** to perform the operation serially, one device after another.

Abort on Failure

Select this checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.

Max Versions

Specify the maximum number of versions to save for this archive. This allows you to limit the number of versions saved for each archive. Once the maximum number is reached, older versions are automatically deleted. If you specify a number that is less than the current number of saved versions, older versions over the maximum number are automatically deleted the next time the archive is performed. Select Unlimited if versions are always retained.

Type

Select the appropriate checkbox for the type of data you wish to archive:

- Archive Configuration Data — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date.
- Archive Capacity Planning Data — Create archives of port and FRU information.

Governance

Select the Run Governance checkbox to perform a governance audit on the archive using the regime you select in the Regime drop-down menu.

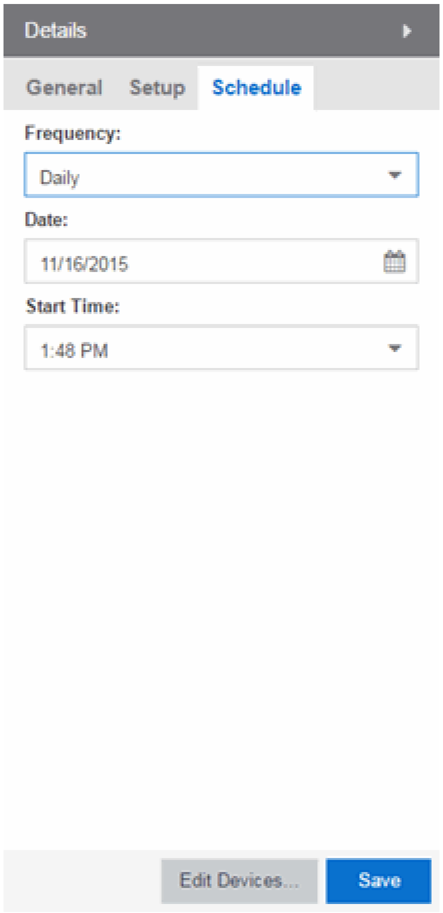
Save

Saves any changes made to the archive attributes. Selecting a Frequency of Now performs the archive immediately.

Edit Devices

Opens the Select Devices window where you can select a single group or a list of devices to include in this archive. This allows you to change the devices the archive is performed on.

Schedule



Frequency: Daily

Date: 11/16/2015

Start Time: 1:48 PM

Frequency

Use the drop-down menu to select the frequency with which you want the archive performed: Never, Now, Once, Daily, Weekly, or On Start Up. The Never option lets you create an archive operation without actually performing it. The Now option lets you perform an immediate archive.

Date

Use the drop-down menu to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by clicking on the calendar. You can use the arrows on either side of the drop-down menu to change the month, and change the year by entering a new year in the text field.

Start Time

Set the starting time for the operation and select AM or PM. (This field is grayed out if you select the Never or Now frequency.)

Related Information

For information on related tabs:

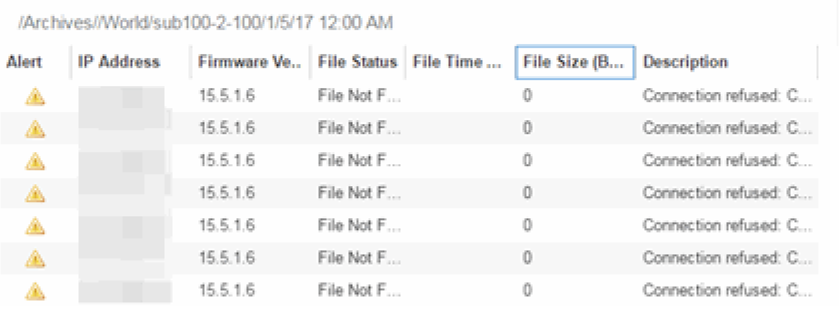
- Archive Name Main Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

Archive Version

The Archive Version panel appears when you select an archive version folder in the left-panel of the **Archive** tab. The archive version is the date and time that an archive operation occurs. The panel displays a table showing the individual configurations saved for this archive version, listed by device IP address. Right-click an item or items in the table for a menu of options.



/Archives//World/sub100-2-100/1/5/17 12:00 AM

Alert	IP Address	Firmware Ve..	File Status	File Time ...	File Size (B...	Description
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...
⚠	[redacted]	15.5.1.6	File Not F...		0	Connection refused: C...

Alert

A yellow alert icon in this column signifies one or more of the following:

- ≠ — Difference between this saved configuration and the previous configuration saved for the same device.
- ⚠ — Configuration save failed.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select Acknowledge Alert from the menu.

IP Address

Lists the individual devices (by device IP address) whose configuration files are saved by this version of the archive operation.

Firmware Version

Shows the firmware version for this device at the time of the save operation.

File Status

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that Extreme Management Center can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data. Check the Description field for more information.

File Time Stamp

The date and time of the configuration creation.

File Size

The size of the saved configuration in bytes.

Description

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. It also displays information pertaining to any alert icon displayed in the Alert column. If the archive did not include a device configuration save, this field displays "Device archived without configuration file." Rest your cursor on the field to display a tooltip of the complete description.

Right-Panel

The right-panel varies depending on whether an archive configuration is selected in the Archive Version main panel table.

- Archive configuration not selected — Archive Version right-panel is displayed.
- Archive configuration is selected — Archive Configuration right-panel is displayed.

Related Information

For information on related tabs:

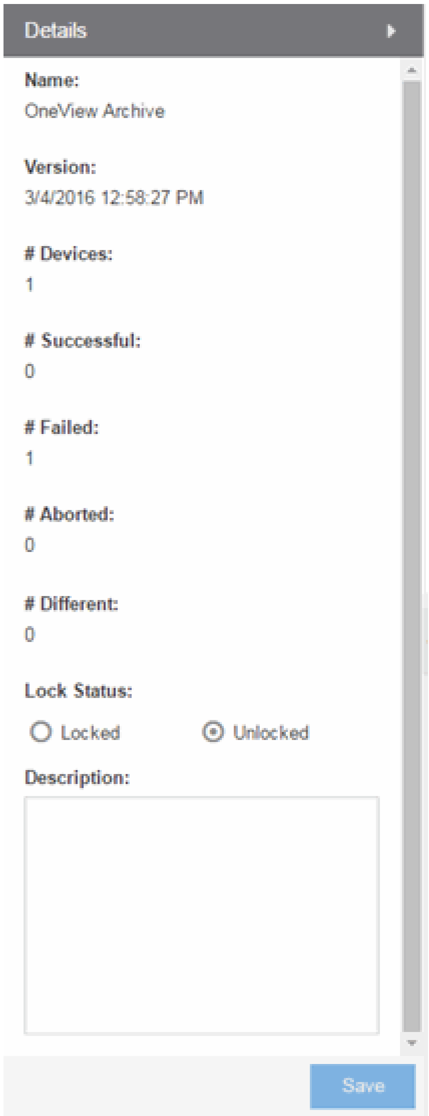
- Archive Version Right-Panel
- Archive File Right-Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

Archive Version (Right-Panel)

The Archive Version right-panel appears when you select an archive version in the left panel of the **Archive** tab or in the table in the Archive Name panel. The archive version is the date and time that an archive operation was performed. This panel displays information about the version, including the number of successful and failed saves for that version.



Name:
OneView Archive

Version:
3/4/2016 12:58:27 PM

Devices:
1

Successful:
0

Failed:
1

Aborted:
0

Different:
0

Lock Status:
○ Locked ● Unlocked

Description:

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

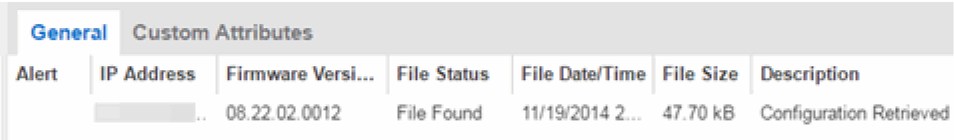
The Archive File panel appears when you select an archive configuration file in the left-panel of the **Archive** tab. It contains information about specific archive configurations.

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	IP Address	Firmware Versi...	File Status	File Date/Time	File Size	Description
	[redacted]	08.22.02.0012	File Found	11/19/2014 2...	47.70 kB	Configuration Retrieved

Alert

A yellow alert icon in this column signifies one or more of the following:

- ≠ — Difference between this saved configuration and the previous configuration saved for the same device.
- ⚠ — Configuration save failed.

To acknowledge an alert and place a checkmark on the alert icon, right-click the icon and select Acknowledge Alert from the menu.

IP Address

Lists the individual devices (by device IP address) whose configuration files were saved by this version of the archive operation.

Firmware Version

Shows the firmware version for this device at the time of the save operation.

File Status

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that Extreme Management Center can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data.

File Time Stamp
The date and time of the configuration creation.

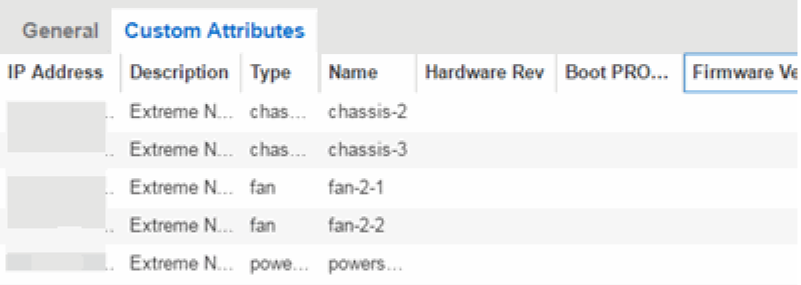
File Size
The size of the saved configuration in bytes.

Description
When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. It also displays information pertaining to any alert icon displayed in the Alert column. If the archive did not include a device configuration save, this field displays "Device archived without configuration file." Rest your cursor on the field to display a tooltip of the complete description.

Custom Attributes Tab

The **Custom Attributes** tab displays a table of attribute information about the selected device(s). The information you see depends on the device type(s) selected; some devices support one attribute but not another. If a device returns multiple values for an attribute, each value is on a separate row. If a device does not support any of the attributes, the **Custom Attributes** tab for that single device is blank.

Custom Attribute tabs for device groups only display devices that support one or more of the attributes. Devices configured with an SNMP context display separate entries for each context.



IP Address	Description	Type	Name	Hardware Rev	Boot PRO...	Firmware Ve
[redacted]	Extreme N...	chas...	chassis-2			
[redacted]	Extreme N...	chas...	chassis-3			
[redacted]	Extreme N...	fan	fan-2-1			
[redacted]	Extreme N...	fan	fan-2-2			
[redacted]	Extreme N...	powe...	powers...			

Description
A description of the module or component.

Type
A description of the module or component type.

Name
The name of the module or component.

Hardware Version
The current hardware version of the device.

BootPROM Version
The current version of Boot PROM installed in the module.

Firmware Version
The current firmware version installed in the module.

Serial Number
A unique number assigned to the module or component by the manufacturer.

Manufacturer
The manufacturer of the module or component.

Model Name
The model number of the module or component type.

Asset Tag
A unique asset number assigned to the module or component for inventory tracking purposes.

Field Replaceable
Whether or not the manufacturer considers the component to be field replaceable (true or false).

Legacy Devices

SSR Hardware Attributes

Slot Number
The slot number in the chassis where the module resides.

Status
The current status of the module: online or offline.

Type
The physical module type.

Description
A description of the module.

Number of Ports
The number of physical ports on the module.

Version

The module version.

Memory

The system memory size available on the module, reported in megabytes (MB).

E5 and E6/E7 Power Supply and Fan Attributes

Power Supply Number

The number of the power supply.

Power Supply Type

The power supply type: ac-dc, dc-dc, or highOutput.

Fan State

The state of the fan: Installed and Operating, Installed and Not Operating, or Not Installed.

Power Supply State

The state of the power supply: Installed and Operating, Installed and Not Operating, or Not Installed.

Power Supply Redundancy

Whether the power supply is redundant or not.

RoamAbout Radiocard and Base MAC Address Attributes

Card Type

The type of PC card inserted in the Access Point.

Versions

The hardware and firmware versions for the PC card.

Station Name

The wireless station name sent out as part of the beacon messages. Valid only when a DS card is inserted in the Access Point.

Base MAC Address

The physical layer address assigned to the interface through which Extreme Management Center is communicating.

Vertical Horizon Attributes

Number in Stack

The total number of switches present on this system.

Number of Ports

The total number of ports present on this system.

Firmware Version

The current firmware version installed in the device.

BootPROM Version

The current version of Boot PROM installed in the device.

CPU

The name of the device's processor (Central Processing Unit).

Power Status

Indicates whether the device is using internal power, redundant power, or both.

Expansion Slot 1

The type of expansion module in slot 1.

Expansion Slot 2

The type of expansion module in slot 2.

Role in System

Indicates whether the device is master, backup master, or slave in the system.

ELS Serial Number Attribute

Serial Number

A unique number assigned to the device by the manufacturer.

Related Information

For information on related windows:

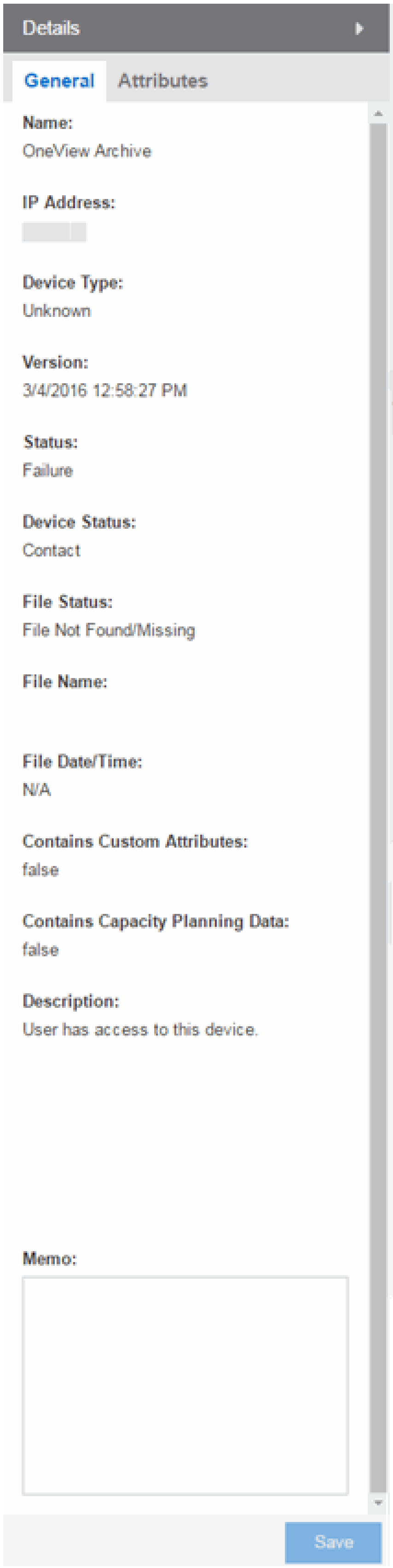
- Archive File Right-Panel

Archive File (Right-Panel)

The Archive File right-panel appears when you select an archive configuration in the left panel of the **Archive** tab or in the table in the Archive Version panel. Each configuration you select contains an icon that identifies the type of data that it contains: device configuration data device configuration data (C) (an individual

.cfg config file), capacity planning data (), or both device configuration and capacity planning data (C). The Archive Configuration right-panel contains two tabs that display information about the saved data.

General



Name:
OneView Archive

IP Address:
[redacted]

Device Type:
Unknown

Version:
3/4/2016 12:58:27 PM

Status:
Failure

Device Status:
Contact

File Status:
File Not Found/Missing

File Name:

File Date/Time:
N/A

Contains Custom Attributes:
false

Contains Capacity Planning Data:
false

Description:
User has access to this device.

Memo:

Name

The name of the archive operation.

IP Address

The IP address of the device whose data is saved, followed by the SNMP context, if applicable.

Device Type

The device's model number or hardware type.

Version

The date and time the archive operation occurred.

Status

The status of the operation: Success or Failure.

Device Status

The status of the device when the archive operation occurred: Contact or No Contact.

File Status

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that Extreme Management Center can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data. Check the Description field for more information.

File Name

The path and filename for the saved configuration. For archive operations configured to archive only capacity planning data (and not configuration data), this column is blank.

File Time Stamp

The date and time of the creation of the configuration file. For archive operations configured to archive only capacity planning data (and not configuration data), this column is blank.

Contains Custom Attributes

Indicates whether the archive contains the device's custom attributes. If the device type does not support custom attributes or if the archive did not complete successfully, this field displays No.

Contains Capacity Planning Data

Indicates whether the device's port and FRU information are saved in the archive.

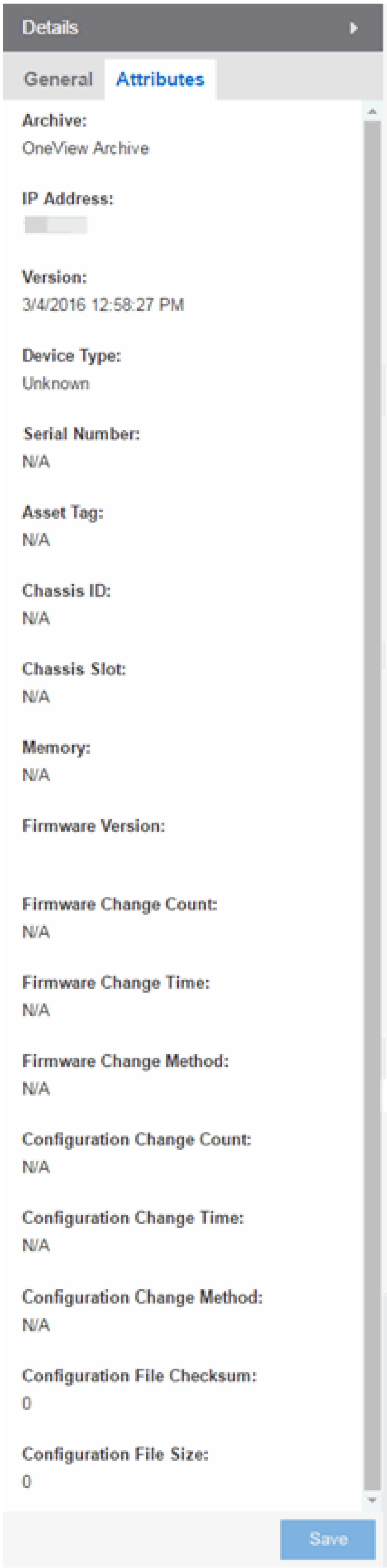
Description

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. For archive operations configured to archive only capacity planning data (and not configuration data), this column displays a Warning message stating that the ability to archive configuration data is disabled for this archive.

Memo

Use this field to add additional notes about the configuration and save them using the Save button.

Attributes



Archive:
OneView Archive

IP Address:
[redacted]

Version:
3/4/2016 12:58:27 PM

Device Type:
Unknown

Serial Number:
N/A

Asset Tag:
N/A

Chassis ID:
N/A

Chassis Slot:
N/A

Memory:
N/A

Firmware Version:

Firmware Change Count:
N/A

Firmware Change Time:
N/A

Firmware Change Method:
N/A

Configuration Change Count:
N/A

Configuration Change Time:
N/A

Configuration Change Method:
N/A

Configuration File Checksum:
0

Configuration File Size:
0

Archive
The name of the archive operation.

IP Address
The IP address of the device whose data is saved, followed by the SNMP context, if applicable.

Version
The date and time that the archive operation occurred.

Device Type
The device's model number or hardware type.

Serial Number
A unique number assigned to the device by the manufacturer.

Asset Tag
A unique asset number assigned to the device for inventory tracking purposes.

Chassis ID
The ID assigned to the chassis where the device resides (if applicable). This is usually a serial number or MAC address, depending on the chassis type.

Chassis Slot
The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

Memory
The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

Firmware Version
The firmware version installed in the device at the time of the configuration save.

Firmware Change Count
The number of successful firmware image downloads. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Firmware Change Time
The date and time of the last successful firmware image download. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Firmware Change Method
The method used to cause the last firmware change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the

source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Count

The number of successful configuration changes. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Time

The date and time of the last successful configuration change. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Method

The method used to make the last configuration change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration File Checksum

The checksum is a value calculated on the entire file. You can compare this value to values obtained from different archive versions. Any difference in checksum values would indicate a change in the configuration.

Configuration File Size

The size of the saved configuration file in bytes. You can compare this size to the size reported in different archive versions. Any difference in size would indicate a change in the configuration file.

Related Information

For information on related tabs:

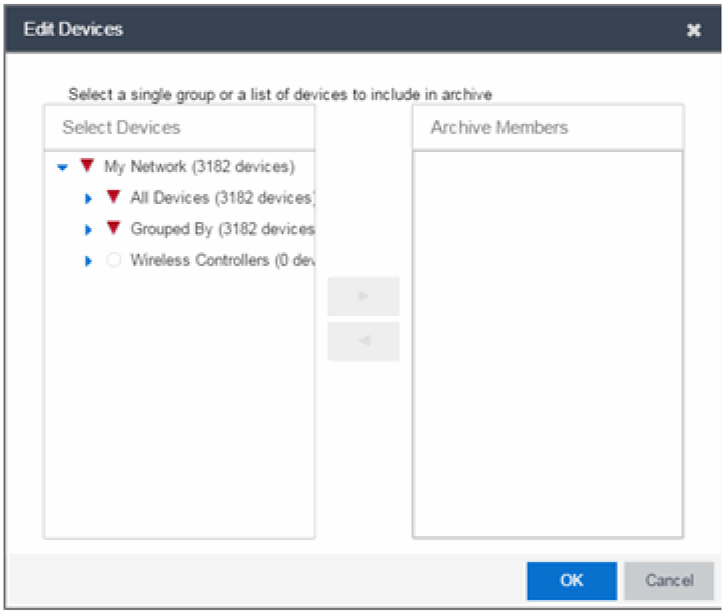
- Archive File Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

Select Devices

This window lets you edit the device(s) on which to perform the archive. The current archive members are listed when you open the window. Access the window from the **Edit Devices** button in the Archive Name right-panel.


Edit Devices
Select a single group or a list of devices to include in archive
Select Devices
My Network (3182 devices)
All Devices (3182 devices)
Grouped By (3182 devices
Wireless Controllers (0 dev
Archive Members
OK
Cancel

Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Click the right arrow button **>** to move the devices to the Archive Members list.

Archive Members

Lists the device(s) or device group the on which the archive is performed. To remove a member from the list, select the member and click the left arrow button **<**.

Right Arrow Button

Click **>** to add the selected device(s) or device group to the Archive Members list.

Remove Button

Click **<** to remove the selected device(s) or device group from the Archive Members list.

OK

Changes the archive members according to your selections.

Related Information

For information on related tabs:

- Archive Name Right-Panel

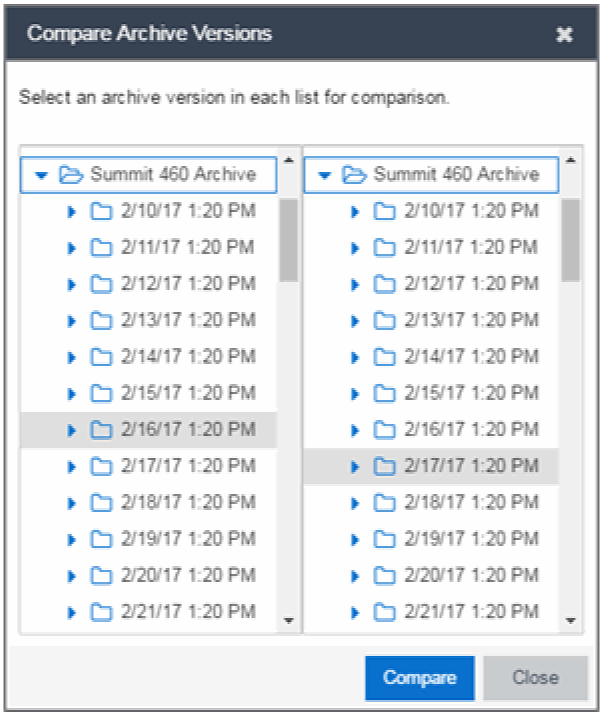
For information on related tasks:

- How to Archive
- How to Compare Archives

Select Archive Versions

This window lets you select two archive versions or configurations to compare in the Compare Archive Versions window. It displays two Archive trees (identical to the Archive tree in the **Archives** tab). Use these trees to select the two archive versions or configuration files you wish to compare. You can compare two individual configurations for the same device, or you can compare two different archive versions (select versions that share common devices).

For information on how to access the window, see How to Compare Archives.



Compare Archive Versions

Select an archive version in each list for comparison.

Selection 1

Expand the folders as necessary to select the first version or configuration you wish to compare.

Selection 2

Expand the folders as necessary to select the second version or configuration you wish to compare.

Compare

Performs the comparison and opens the Compare Archive Versions window, where you can view the comparison results.

Close

Closes the window.

Related Information

For information on related windows:

- Compare Configuration Files Window
- Configuration File Viewer

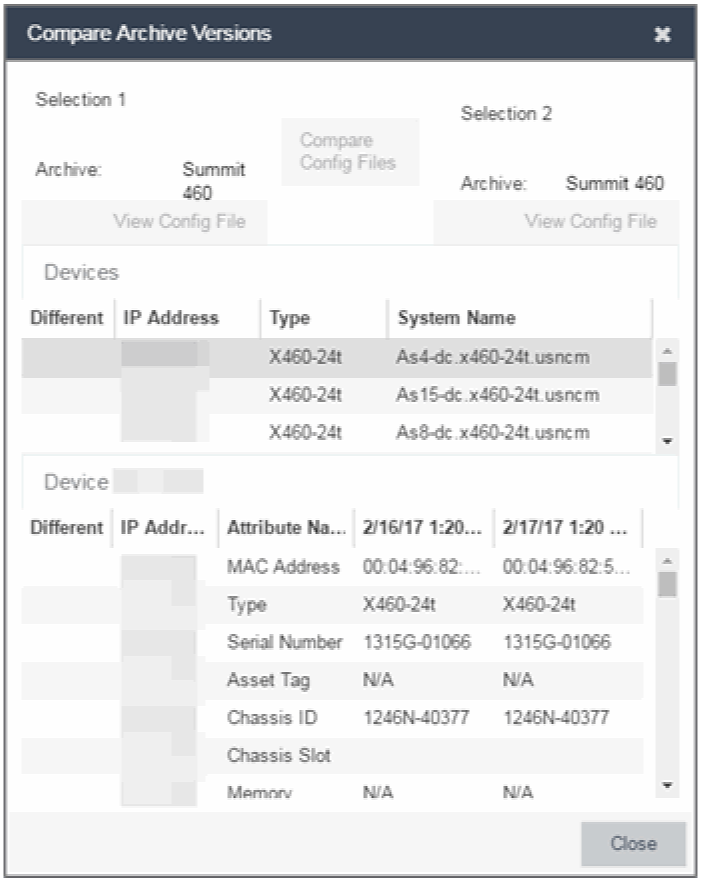
For information on related tasks:

- How to Archive
- How to Compare Archives

Compare Archive Versions

The Compare Archives window lets you compare two different archives for the same device and monitor any changes in device attributes. Extreme Management Center compares archives using a set group of saved attributes from when the archive occurred. The values for these attributes are displayed in a table with any differences between the values flagged by a yellow **Diff** icon ≠ in the **Different** column.

For information on how to perform a compare archive operation, see How to Compare Archives.



Selection 1

Archive: Summit 460

Selection 2

Archive: Summit 460

Devices

Different	IP Address	Type	System Name
	[redacted]	X460-24t	As4-dc.x460-24t.usncm
	[redacted]	X460-24t	As15-dc.x460-24t.usncm
	[redacted]	X460-24t	As8-dc.x460-24t.usncm

Device [redacted]

Different	IP Addr...	Attribute Na...	2/16/17 1:20...	2/17/17 1:20 ...
	[redacted]	MAC Address	00:04:96:82:...	00:04:96:82:5...
	[redacted]	Type	X460-24t	X460-24t
	[redacted]	Serial Number	1315G-01066	1315G-01066
	[redacted]	Asset Tag	N/A	N/A
	[redacted]	Chassis ID	1246N-40377	1246N-40377
	[redacted]	Chassis Slot		
	[redacted]	Memory	N/A	N/A

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.

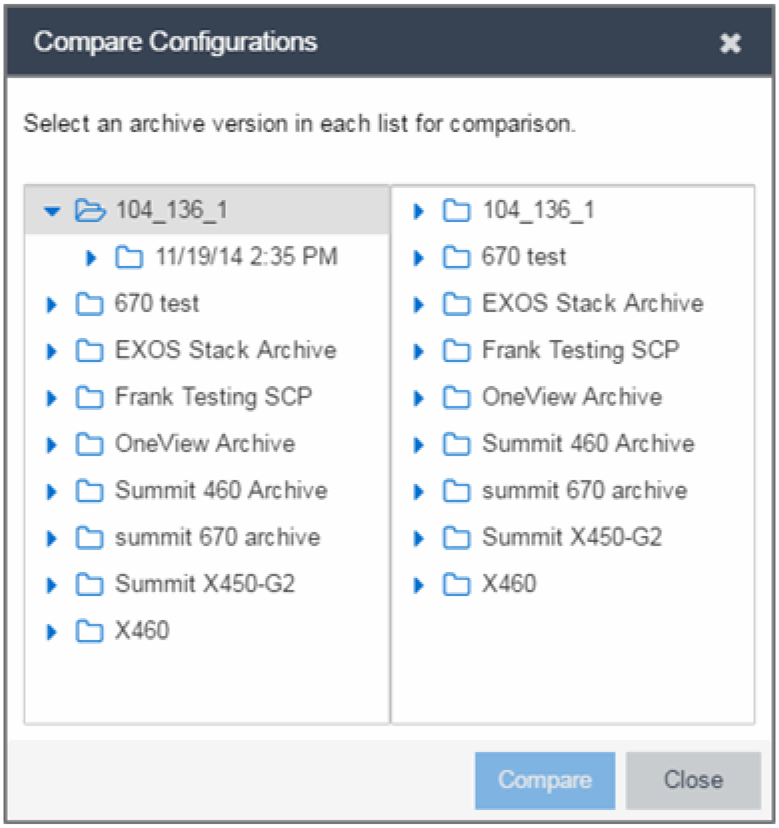
Related Information

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 (C or C) in the **Archives** tab tree or main panel, and select **Compare Configuration Files**.



Compare Configurations

Select an archive version in each list for comparison.

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

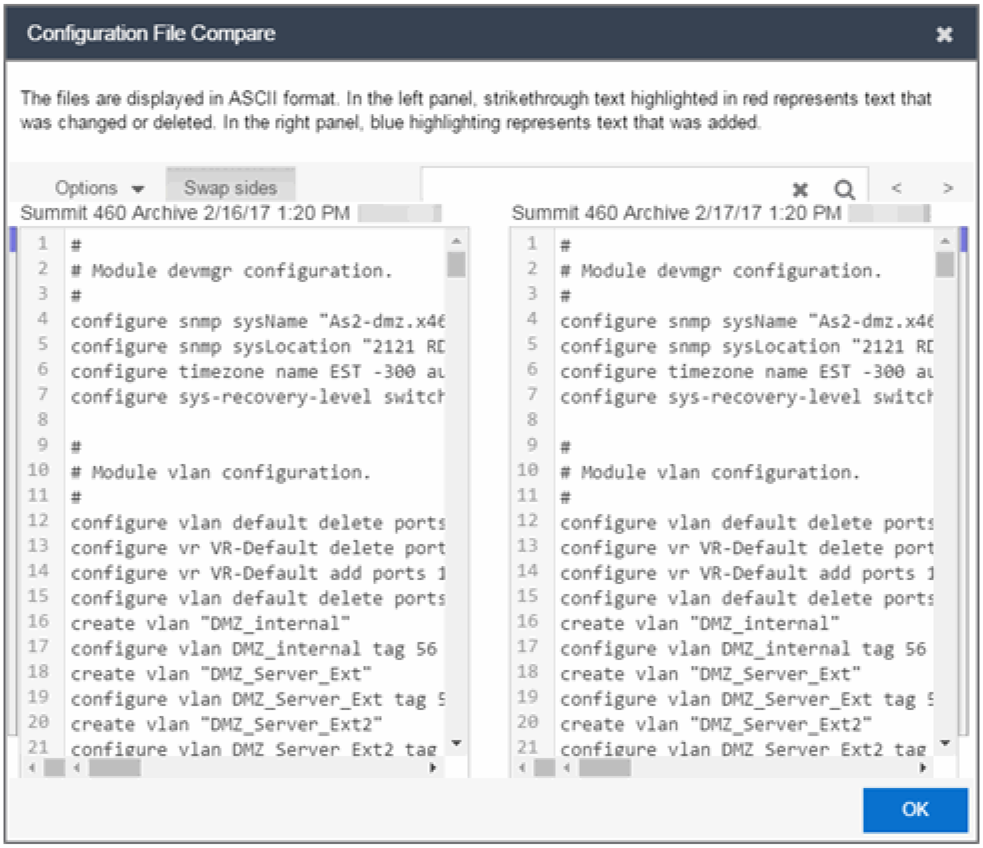
Configuration File Compare

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 (C 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.



The files are displayed in ASCII format. In the left panel, strikethrough text highlighted in red represents text that was changed or deleted. In the right panel, blue highlighting represents text that was added.

Summit 460 Archive 2/16/17 1:20 PM

```
#
# Module devmgr configuration.
#
configure snmp sysName "As2-dmz.x46
configure snmp sysLocation "2121 RD
configure timezone name EST -300 au
configure sys-recovery-level switch

#
# Module vlan configuration.
#
configure vlan default delete ports
configure vr VR-Default delete port
configure vr VR-Default add ports 1
configure vlan default delete ports
create vlan "DMZ_internal"
configure vlan DMZ_internal tag 56
create vlan "DMZ_Server_Ext"
configure vlan DMZ_Server_Ext tag 5
create vlan "DMZ_Server_Ext2"
configure vlan DMZ_Server_Ext2 tag
```

Summit 460 Archive 2/17/17 1:20 PM

```
#
# Module devmgr configuration.
#
configure snmp sysName "As2-dmz.x46
configure snmp sysLocation "2121 RD
configure timezone name EST -300 au
configure sys-recovery-level switch

#
# Module vlan configuration.
#
configure vlan default delete ports
configure vr VR-Default delete port
configure vr VR-Default add ports 1
configure vlan default delete ports
create vlan "DMZ_internal"
configure vlan DMZ_internal tag 56
create vlan "DMZ_Server_Ext"
configure vlan DMZ_Server_Ext tag 5
create vlan "DMZ_Server_Ext2"
configure vlan DMZ_Server_Ext2 tag
```

Search

Use the **Search** box at the top of the window to search for strings of characters in the configuration files.

Clear Search Button ⊗

Click this button to clear the search parameters from the **Search** box.

Find Previous Row/Find Next Row Buttons < >

Click these buttons to find the previous or next row that contains search parameters that match what you entered in the **Search** box.

Swap Sides Button Swap sides

Clicking this button switches the sides on which each archive configuration is located.

Options Options

The **Options** drop-down menu allows you to configure how information displays in the archive configurations.

- **Enable line numbers** — Select this checkbox to display line numbers to the left of each line in the configuration file.
- **Wrap lines** — Select this checkbox to wrap text in the configuration files, so a horizontal scroll bar is not required to view information.
- **Enable side bars** — Select this checkbox to display a sidebar on the outside of each configuration file indicating your relative position in the file.

OK

Click the **OK** button to close the Configuration File Compare window and return to the previous screen.

Related Information

For information on related windows:

- Configuration File Viewer

For information on related tasks:

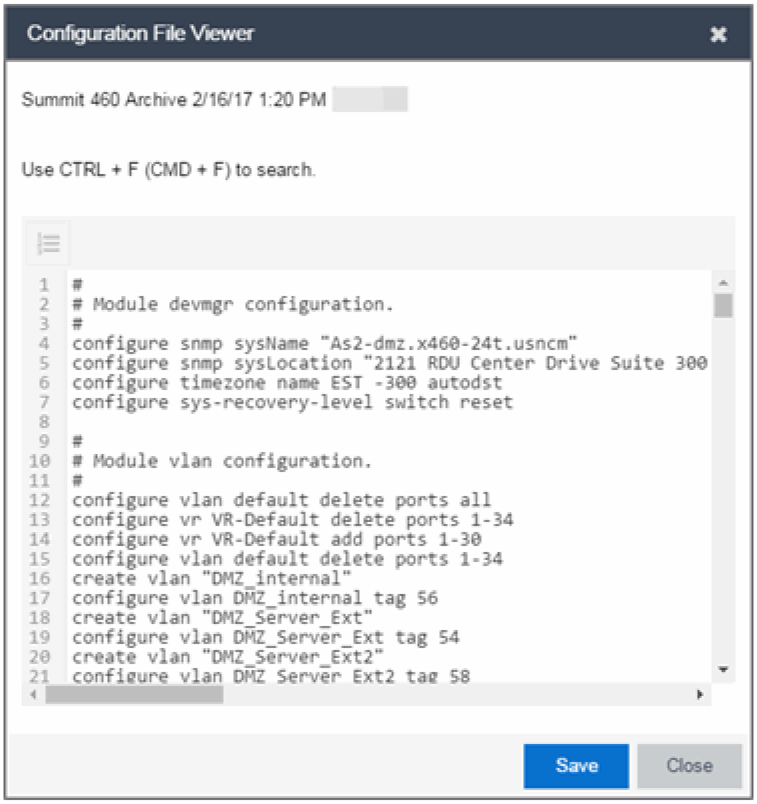
- How to Archive
- How to Compare Archives

Configuration File Viewer

The Configuration File Viewer lets you view an archived device configuration file. To access the viewer, select a configuration that includes device configuration data (c or C) 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.



Summit 460 Archive 2/16/17 1:20 PM

Use CTRL + F (CMD + F) to search.

```
#
# Module devmgr configuration.
#
configure snmp sysName "As2-dmz.x460-24t.usncm"
configure snmp sysLocation "2121 RDU Center Drive Suite 300
configure timezone name EST -300 autodst
configure sys-recovery-level switch reset

#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-34
configure vr VR-Default add ports 1-30
configure vlan default delete ports 1-34
create vlan "DMZ_internal"
configure vlan DMZ_internal tag 56
create vlan "DMZ_Server_Ext"
configure vlan DMZ_Server_Ext tag 54
create vlan "DMZ_Server_Ext2"
configure vlan DMZ Server Ext2 tag 58
```

Save

Click **Save** to automatically save the configuration file to your default download folder in CFG format.

Close

Click **Close** to exit the Configuration File Viewer window and return to the previous screen.

Related Information

For information on related windows:

- Configuration File Compare Window

For information on related tasks:

- How to Archive
- How to Compare Archives

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, Extreme Management Center generates an event log message. Using the Extreme Management Center **Alarms & Events** tab, you can create an alarm that monitors the log for the text "Configurations Are Different" and define an e-mail to be executed as the specific alarm action.

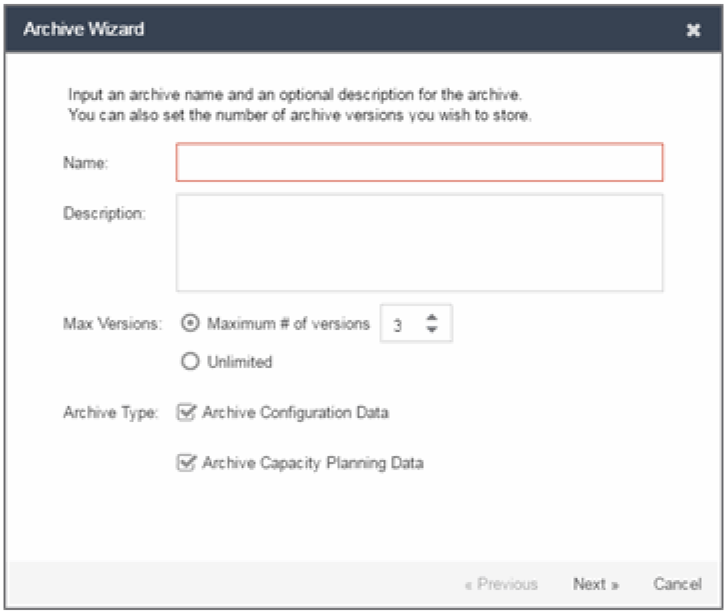
Once an archive operation is created, it is listed by name in the left-panel Archives folder. Below the archive name are the archive versions, displayed by the date and time of the creation of the version. Under the versions are individual configurations, listed by the IP address of the device whose data is saved. Each configuration displays an icon that identifies the type of data being saved: device configuration data (C), capacity planning data (▥), both device configuration and capacity planning data (C▥).

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.



Input an archive name and an optional description for the archive.
You can also set the number of archive versions you wish to store.

Name:

Description:

Max Versions: ● Maximum # of versions 3
○ Unlimited

Archive Type: ☑ Archive Configuration Data
☑ Archive Capacity Planning Data

Name

Enter a name for the archive operation.

Description

Enter a description *(optional)* of the archive operation.

Archive Setup

Max Versions

If desired, specify the maximum number of versions saved for this archive. This allows you to limit the number of versions saved for each archive. Once the maximum number is reached, Extreme Management Center automatically deletes older versions. Otherwise, select **Unlimited** to continue adding archive versions with no limit.

Archive Type

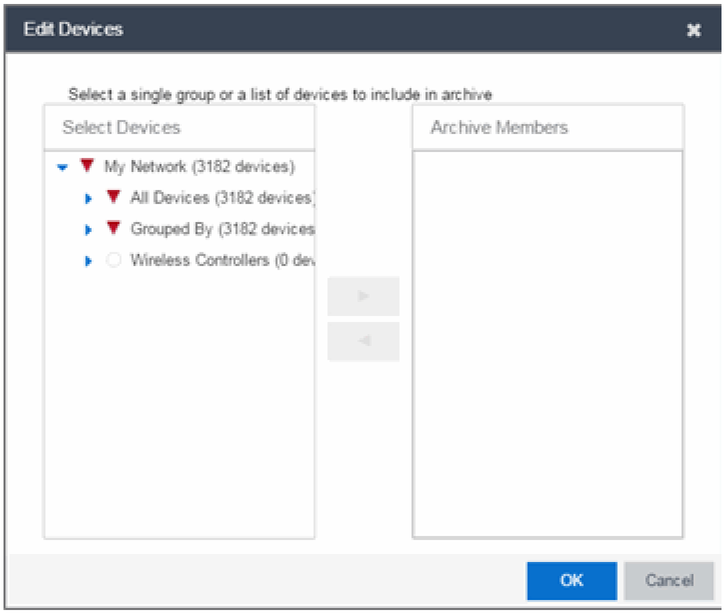
Select the appropriate checkbox for the type of data you wish to archive:

- Archive Configuration Data — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date.
- Archive Capacity Planning data — Create archives of port and FRU information.

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.)



Edit Devices

Select a single group or a list of devices to include in archive

Select Devices
My Network (3182 devices)
All Devices (3182 devices)
Grouped By (3182 devices
Wireless Controllers (0 dev
Archive Members
>
<
OK
Cancel

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

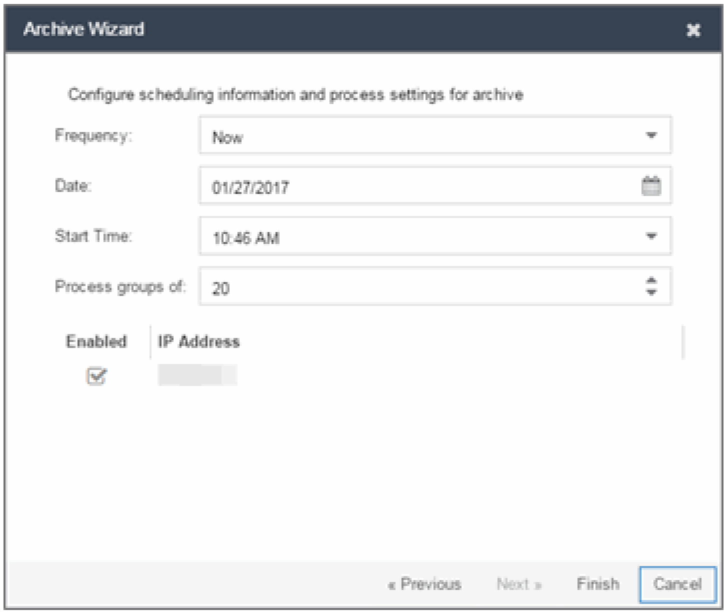
In the Devices tree, select the device(s) or device group you want to archive, and click **>** to add it to the Archive Members list.

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.



Configure scheduling information and process settings for archive

Frequency: Now

Date: 01/27/2017

Start Time: 10:46 AM

Process groups of: 20

Enabled	IP Address
☑	[redacted]

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

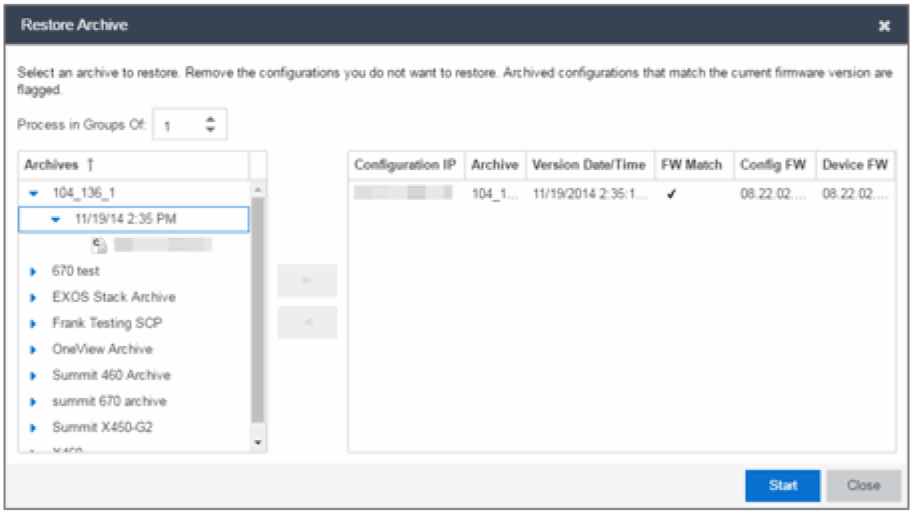
Use the Restore Wizard to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel of the Archive tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of saved data: device configuration data (C), capacity planning data (▤), both device configuration and capacity planning data (C▤). Only configurations that include device configuration data (C and C▤) 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, right-click an archive version or an archive configuration from the left-panel of the **Archive** tab or from the main panel and select **Restore**.

Archive Version Selection Window

Use this window to select an archive version or single configuration to restore. Select the archive version or configuration in the Archives list and click the right arrow button **>** to move it to the restore list. If you select an archive version, use the left arrow button **<** to remove any individual configurations included in the archive version you do not wish to restore.



Select an archive to restore. Remove the configurations you do not want to restore. Archived configurations that match the current firmware version are flagged.

Process in Groups Of: 1

Configuration IP	Archive	Version Date/Time	FW Match	Config FW	Device FW
[redacted]	104_1...	11/19/2014 2:35:1...	✓	08.22.02....	08.22.02....

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 (C), capacity planning data (▯), both device configuration and capacity planning data (C▯). Only configurations that include device configuration data (C and C▯) 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 restart automatically restart after the restore is complete.

Show all devices/Show only incomplete and failed

Once the restore operation starts, the device list table updates with status information for each device. An alert icon (⚠) appears in the Alert column of the table if a restore operation fails for a specific device. Use these radio buttons to show all devices or show only those devices whose restore operations are incomplete or failed.

Device List Table

A list of the devices you selected for your restore operation. Once the restore is started, this table updates with status information for the restore operation:

- Alert — an alert icon ⚠ appears in the Alert column if a restore operation fails for a specific device.
- IP Address — The device's IP address. Chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- Configuration — The name of the configuration file being restored.
- Status — The status of the operation for that particular device: Success or Failure.
- Operation — The type of operation performed: Configuration Restore.
- % Progress — A progress bar showing the percent completed of the operation.
- Bytes Trans. — The number of bytes transferred during the operation.
- Message — A message relating to the status of the operation.

Status Summary

Once the restore is started, this area updates with status information for the restore operation.

Restore Type

The restore is performed in parallel (simultaneously) on the number of devices specified in the Process 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 restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. Use a Process groups of value of 1 (perform the restore serially,) unless you know it is safe for the selected network devices to restart simultaneously.

Start Button

Initiates the restore operation. The table at the top of the window and the status area in the bottom left of the window update with status information.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive

How to Archive

You can archive (save) device configuration data and/or capacity planning data using the Archive Wizard. Archiving device configuration data lets you create archives (backup copies) of your network devices' configurations you can restore to the devices at a later date. Archiving capacity planning data lets you store port and FRU information. You can create an archive that saves both configuration data and capacity planning data, or you can create an archive that targets one type of data or the other.

You can perform archives on a single device, multiple devices, or on an entire device group. Because it is useful to archive data on a regular basis, Extreme Management Center lets you schedule archives to be performed at a future time, and/or on a routine basis. Once you configure an archive's parameters, you can use that archive on a repeated basis to save new versions of the desired data. For example, you can create an archive that saves your device configurations on a weekly basis, and also create an archive that saves only capacity planning information on a daily basis to monitor what is changing on the network.

Once 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 (c), capacity planning data (▯), or both device configuration and capacity planning data (c▯).

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:

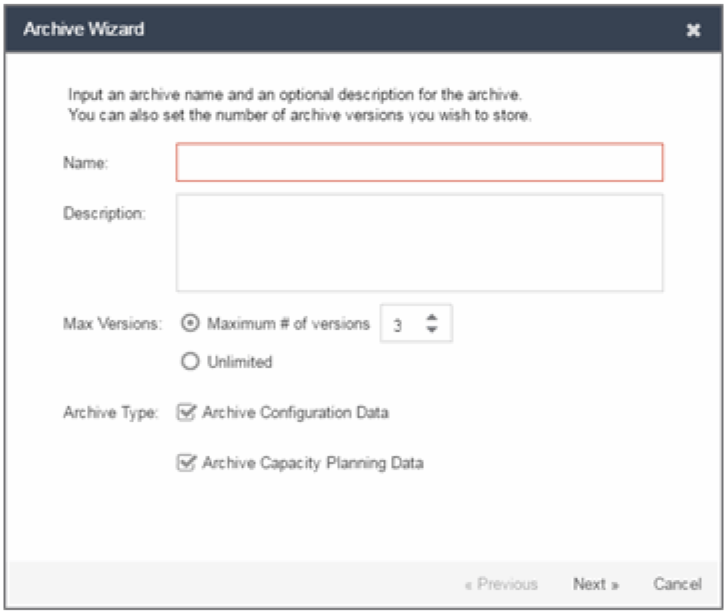
- Using the Archive Wizard
- Saving a New Archive Version
- Editing an Archive

- [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.



Archive Wizard

Input an archive name and an optional description for the archive.
You can also set the number of archive versions you wish to store.

Name:

Description:

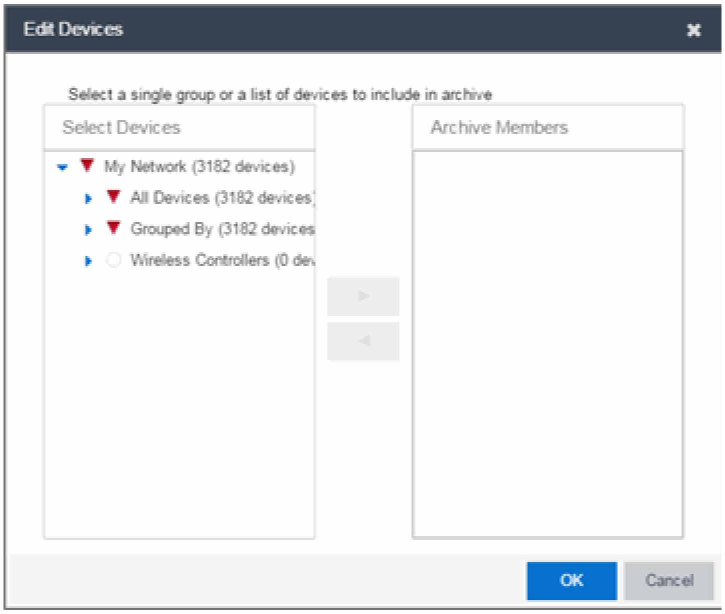
Max Versions: ● Maximum # of versions 3
○ Unlimited

Archive Type: ☑ Archive Configuration Data
☑ Archive Capacity Planning Data

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 used to generate reports.

c. Click **Next**.
The next Select Devices window appears.



Edit Devices

Select a single group or a list of devices to include in archive

Select Devices
My Network (3182 devices)
All Devices (3182 devices)
Grouped By (3182 devices
Wireless Controllers (0 dev
Archive Members
OK
Cancel

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.

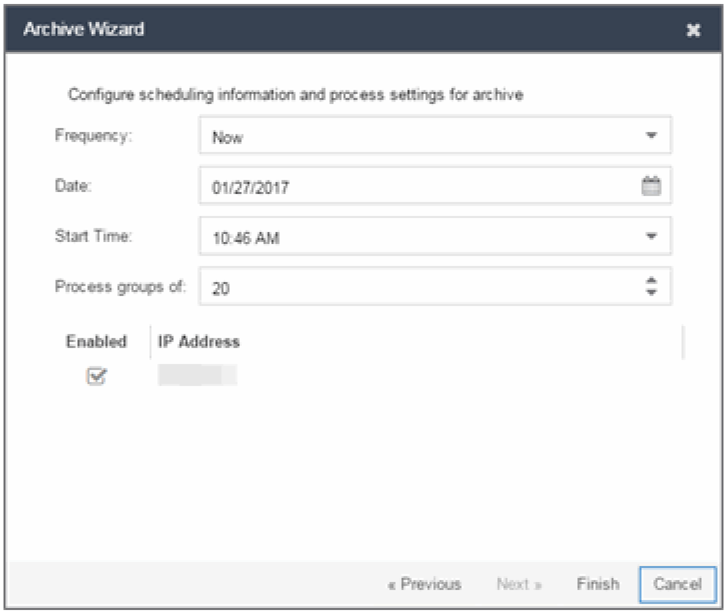
NOTE: If you select multiple tree nodes representing the same device, but with varying SNMP contexts, an archive save is performed for each context. However, the context must provide access to the MIBs required for the archive save operation or the archive for that context fails. It is recommended you 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.



Archive Wizard

Configure scheduling information and process settings for archive

Frequency: Now

Date: 01/27/2017

Start Time: 10:46 AM

Process groups of: 20

Enabled	IP Address
☑	[redacted]

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, Extreme Management Center generates an event log message.

Saving a New Archive Version

Once you create an archive, use that archive on a repeated basis to save (stamp) new versions of the desired configurations.

1. With an archive folder selected in the left-panel **Archives** tab, right-click and select **Stamp New Version** from the menu.
2. A new archive version, displayed by the date and time the version is performed, is listed under the archive folder. Under the version are the individual configurations, listed by the IP address of the saved device.

Editing an Archive

Once you create an archive, you can edit the archive parameters, including changing the devices on which the archive is performed.

1. 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 Compare Archives

Extreme Management Center lets you compare two different archives for the same device and monitor any changes in device attributes. Extreme Management Center compares archives using a set group of attributes you saved when the archive was performed. The values for these attributes appear in a table with any differences between the values flagged by a yellow **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

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 (C), capacity planning data (▯), both device configuration and capacity planning data (C▯). Only configurations that include device configuration data (C and C▯) 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 (C and C) 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 restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. It is recommended you leave the **Process groups of** value at 1 (perform the restore serially), unless you know it is safe to the simultaneously restart the selected network devices.

   b. Click **Start** to initiate the restore operation. The table at the top of the window and the status area in the bottom left of the screen both update with status information.

   c. Review results. An alert icon (⚠) appears in the Alert column of the table if a restore operation fails for a specific device. You can select to show all devices or show only incomplete or failed device archive restorations.

4. Click **Finish** to close the wizard.

Related Information

For information on related tasks:

- Restore Wizard
- How to Archive

How to Back up, Restore, and Compare Device Configurations in Extreme Management Center

You can back up (archive) and restore device configurations as well as compare two configuration files, using the **Network** tab in Extreme Management Center. The backup operation performs a single configuration archive. The restore operation restores an archived configuration or configuration template to a device. The compare operation compares the last two archived configuration files for a selected device.

All of the operations require that you are using the Archives tab for your archive management.

Device Back up Configuration

To perform a quick device configuration back up (archive) without going into the **Archives** tab:

1. Select a device in the Device list.
2. Click the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Configuration/Firmware** > **Backup Configuration**.

   This performs a single configuration archive for the device. You can refer to the Extreme Management Center Inventory Event Log to view the archive progress.
4. Open the **Network** > **Archives** tab to view the archive.

NOTES: To perform the backup configuration, you must be a member of an authorization group that has the Inventory Manager > Configuration Archive Management > Archive Restore Wizard capability.

Because the Extreme Management Center backup creates a single archive that is not recurring, use the Archive Wizard on the **Archives** tab to schedule regular backups of your network device configurations.

Device Restore Configuration

The device restore configuration operation allows you to restore a configuration template or archived configuration to an active device on the network.

1. Select a device in the Device list.
2. Click the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Configuration/Firmware** > **Restore Configuration**.

   For additional information about restoring a device's configuration, see Restore Device Configuration in Extreme Management Center.

Compare Device Configurations

You can compare the last two archived configuration files for a selected device, without going into the **Archives** tab.

1. Select a device in the Device list.
2. Click the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Configuration/Firmware** > **Compare Last Configurations**.

   For additional information about comparing device configurations, see Compare Device Configurations in Extreme Management Center.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware Tab

Alarms & Events

The **Alarms & Events** tab displays alarm and event details for all managed devices in the network, with sorting and filtering of relevant information for network troubleshooting and forensics.

Additionally, the **Menu** icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

This Help topic provides information on the following topics:

- Access Requirements
- Alarms
- Alarm Configuration
- Events
    - Event Log Column Definitions
- Buttons, Search Field, and Paging Toolbar

Access Requirements

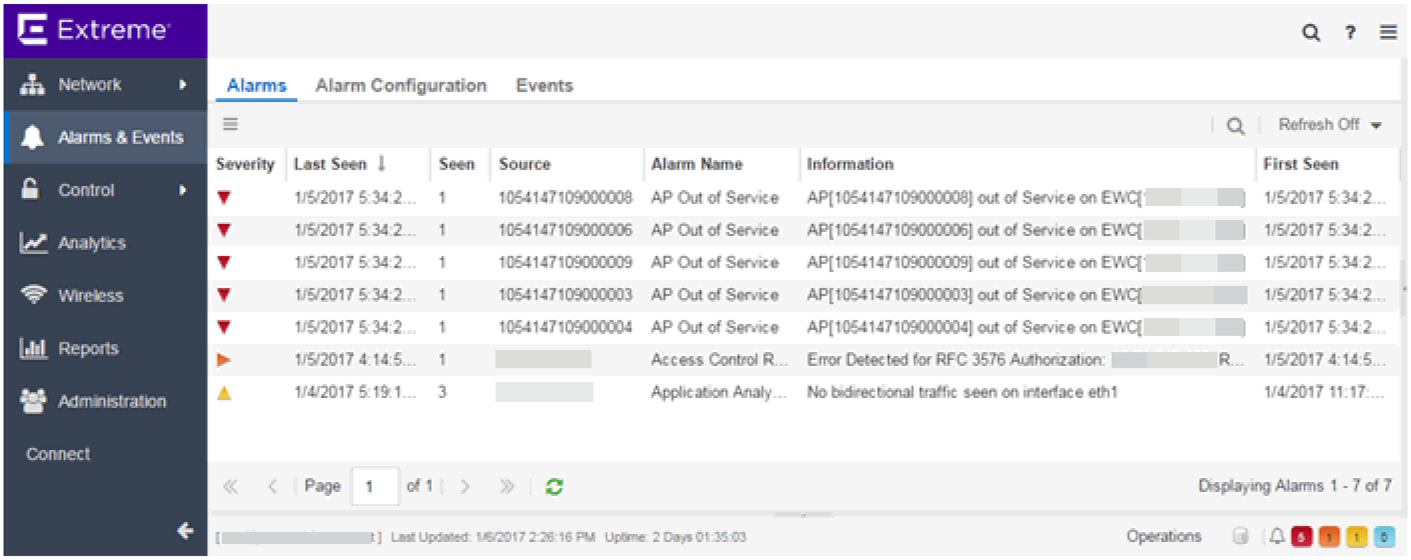
To view the information in the Alarms and Event logs, you must be a member of an authorization group assigned the appropriate Extreme Management Center capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read Access or Read/Write Access

For additional information, see Users and Extreme Management Center Access Requirements.

Alarms

Use the **Alarms & Events** tab to access the **Alarms** tab that displays the current alarms for the network.



Severity	Last Seen	Seen	Source	Alarm Name	Information	First Seen
▼	1/5/2017 5:34:2...	1	1054147109000008	AP Out of Service	AP[1054147109000008] out of Service on EWC[[redacted]]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000006	AP Out of Service	AP[1054147109000006] out of Service on EWC[[redacted]]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000009	AP Out of Service	AP[1054147109000009] out of Service on EWC[[redacted]]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000003	AP Out of Service	AP[1054147109000003] out of Service on EWC[[redacted]]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000004	AP Out of Service	AP[1054147109000004] out of Service on EWC[[redacted]]	1/5/2017 5:34:2...
▶	1/5/2017 4:14:5...	1	[redacted]	Access Control R...	Error Detected for RFC 3576 Authorization: [redacted] R...	1/5/2017 4:14:5...
▲	1/4/2017 5:19:1...	3	[redacted]	Application Analy...	No bidirectional traffic seen on interface eth1	1/4/2017 11:17:...

Page 1 of 1

Displaying Alarms 1 - 7 of 7

[[redacted]] Last Updated: 1/6/2017 2:26:16 PM Uptime: 2 Days 01:35:03

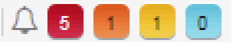
Operations 5 1 1 0

In the **Alarms** tab:

- Right-click on the alarm or click the **Menu** icon (☰) and select **Alarm History** > **By Source** to view an Alarm History for that device. If the Source includes a subcomponent (such as an interface on the device), then the alarm history is specific to that subcomponent.
- Right-click on the alarm column or click the **Menu** icon (☰) and select **Alarm History** > **By Alarm Name** to view an Alarm History for a specific alarm.
- Right-click on the alarm or click the **Menu** icon (☰) and select **Alarm History** > **All** to view the Alarm History for all devices.
- Right-click on an alarm to clear the selected alarm or to clear all alarms. Supply a reason the alarm cleared, if necessary. which is recorded in the Alarm History.
- Right-click on an alarm or select an alarm and click the **Menu** icon (☰) and select **Edit Alarm Definition** to open the alarm in the Alarm Configuration window, from which you can edit the criteria which triggers the alarm.
- Double-click on any row in the table to open a window that displays Alarm Details.

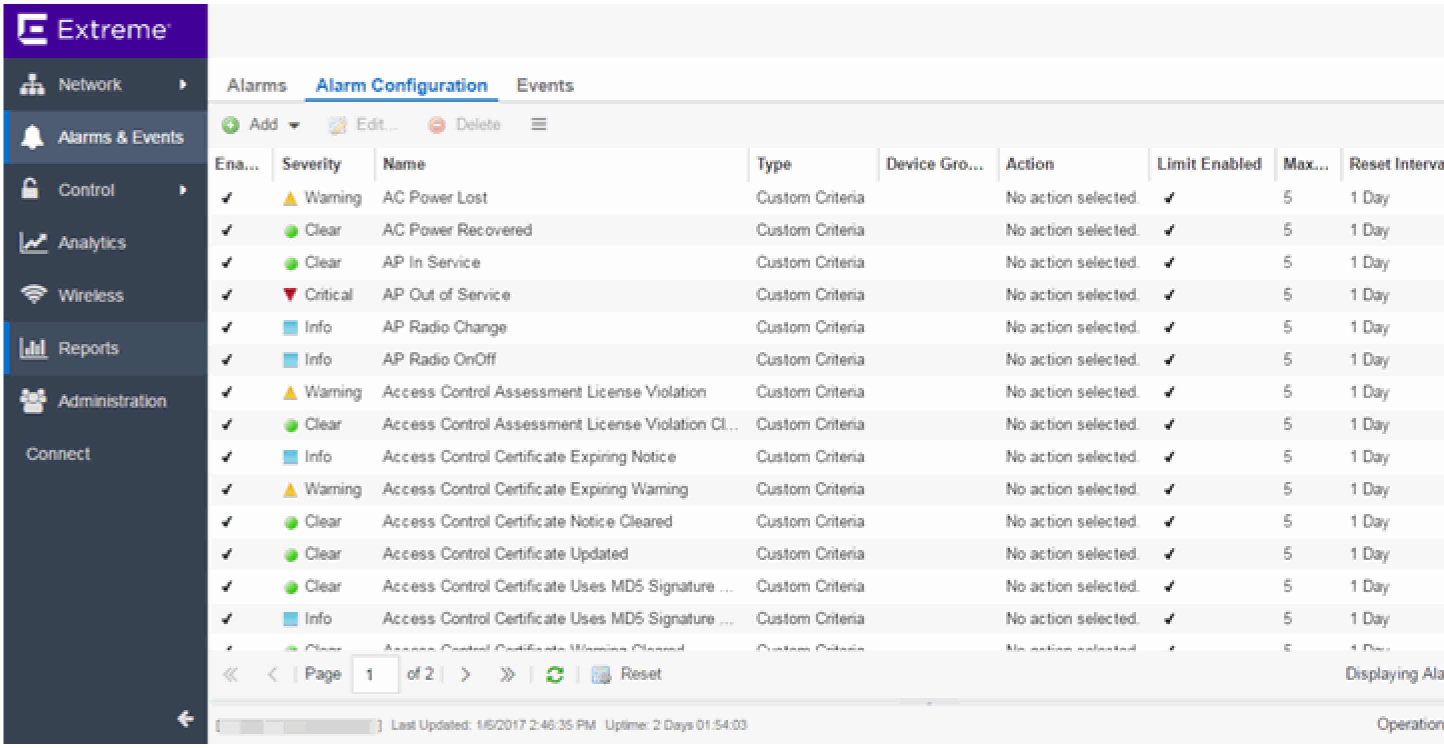
Alarm Summary

Every Extreme Management Center page includes a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) present in the entire system. If there are no current alarms, the status displays all zeroes. Click on an indicator to open the **Alarms** tab filtered to display the alarms of that severity. An alarm with a slash indicates the alarm is disabled.



Alarm Configuration

The **Alarm Configuration** tab in the **Alarms & Events** tab allows you to configure the network alarms that provide status information for a particular problem or condition on a particular network component. Alarms are triggered when event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed. From the **Alarm Configuration** tab you can also create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Link Down alarm is triggered when a device emits a linkDown trap. Then, when the device emits a linkUp trap, the Link Up alarm automatically clears the Link Down alarm.



Ena...	Severity	Name	Type	Device Gro...	Action	Limit Enabled	Max...	Reset Interva
✓	Warning	AC Power Lost	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	AC Power Recovered	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	AP In Service	Custom Criteria		No action selected.	✓	5	1 Day
✓	Critical	AP Out of Service	Custom Criteria		No action selected.	✓	5	1 Day
✓	Info	AP Radio Change	Custom Criteria		No action selected.	✓	5	1 Day
✓	Info	AP Radio OnOff	Custom Criteria		No action selected.	✓	5	1 Day
✓	Warning	Access Control Assessment License Violation	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	Access Control Assessment License Violation Cl...	Custom Criteria		No action selected.	✓	5	1 Day
✓	Info	Access Control Certificate Expiring Notice	Custom Criteria		No action selected.	✓	5	1 Day
✓	Warning	Access Control Certificate Expiring Warning	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	Access Control Certificate Notice Cleared	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	Access Control Certificate Updated	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	Access Control Certificate Uses MD5 Signature ...	Custom Criteria		No action selected.	✓	5	1 Day
✓	Info	Access Control Certificate Uses MD5 Signature ...	Custom Criteria		No action selected.	✓	5	1 Day
✓	Clear	Access Control Certificate Warning Cleared	Custom Criteria		No action selected.	✓	5	1 Day

Last Updated: 1/6/2017 2:46:35 PM Uptime: 2 Days 01:54:03

Via the **Add** menu, you can:

- Add a new alarm definition, which includes configuring the conditions (criteria) that trigger the alarm, and defining the actions that occur automatically to notify a person or network component about the problem, when the alarm triggers.

- Edit and delete alarm definitions as well as configure email settings for alerts.

Extreme Management Center ships with a set of default alarm definitions, which you can use as is, or delete or modify them as desired.

Alarm Configuration Column Definitions

Enabled — A checkmark in the Enabled column indicates the alarm definition is active. Ignore an alarm definition to ignore your enabled alarms without deleting the definition.

Severity — This column indicates the seriousness of an alarm definition, which posses its own specified severity regardless of the severity of the event or trap that triggered it.

- ? (question mark) Set from Source — the alarm definition uses the severity level of the trigger event, for example a warning event.
- ▼ (Red) Critical — A problem with significant implications.
- ▶ (Orange) Error — A problem with limited implications.
- ▲ (Yellow) Warning — A condition that might lead to a problem.
- ■ (Blue) Info — Information only; not a problem.
- ● (Green) Clear — An alarm that clears another alarm (for example, LinkUp).

Name — The name of the alarm definition.

Type — Identifies the type of alarm definition for this row (threshold, trap, or custom criteria).

Device Groups — If desired, you can restrict the alarm definition to devices and port elements in one or more device groups. This column indicates the device group to which the alarm definition is assigned. The alarm definition is only raised on the devices and interfaces in the selected device groups. This allows you to filter alarms to specific devices or important ports.

Action — The actions that occur when an alert is triggered, if any.

Limit Enabled — A checkbox indicates that there is a rate-limit on the alarm's actions.

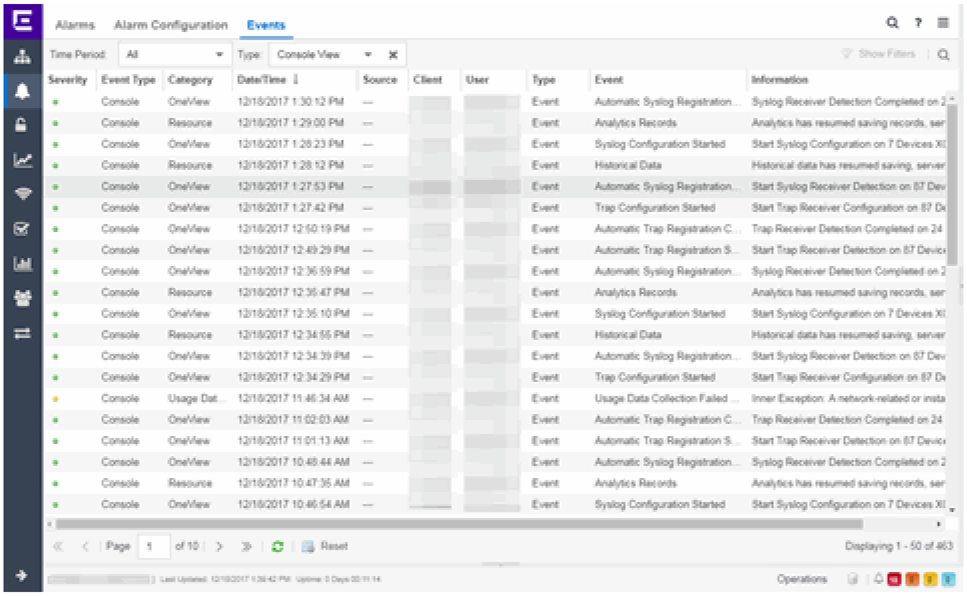
Max Count — If Limit Enabled is checked, this column indicates the number of times an action is performed for this alarm. Once the limit is reached, the alarm is still recorded, but no further actions are performed until the Reset Interval expires. If you configure multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. If Limit Enabled is not checked, there is no limit placed on the number of times the action is performed.

Reset Interval — If Limit Enabled is checked, this column displays the length of time from when the first action is triggered until the count is reset. Once the count is reset, actions are executed until the Max Count is reached again. If the reset interval is set to "None", then once the alarm limit is reached, the alarm does not reset unless manually reset.

Clearing Alarms — This column displays the **Name** of the alarm that acts to clear the current alarm.

Events

Open the **Events** tab in the **Alarms & Events** tab to access the event log, as well as the event logs for Extreme Management Center, legacy applications, and Extreme Access Control Audit events and Wireless Audit events. In addition, you can access an event log for Extreme Management Center Scheduler events.



Time Period: All
Type: Console View

Severity	Event Type	Category	Date/Time	Source	Client	User	Type	Event	Information
●	Console	OneView	12/18/2017 1:30:12 PM	—	[redacted]	[redacted]	Event	Automatic Syslog Registration...	Syslog Receiver Detection Completed on 2
●	Console	Resource	12/18/2017 1:29:00 PM	—	[redacted]	[redacted]	Event	Analytics Records	Analytics has resumed saving records, ser
●	Console	OneView	12/18/2017 1:28:23 PM	—	[redacted]	[redacted]	Event	Syslog Configuration Started	Start Syslog Configuration on 7 Devices X(
●	Console	Resource	12/18/2017 1:28:12 PM	—	[redacted]	[redacted]	Event	Historical Data	Historical data has resumed saving, server
●	Console	OneView	12/18/2017 1:27:53 PM	—	[redacted]	[redacted]	Event	Automatic Syslog Registration...	Start Syslog Receiver Detection on 87 Dev
●	Console	OneView	12/18/2017 1:27:42 PM	—	[redacted]	[redacted]	Event	Trap Configuration Started	Start Trap Receiver Configuration on 87 De
●	Console	OneView	12/18/2017 12:50:19 PM	—	[redacted]	[redacted]	Event	Automatic Trap Registration C...	Trap Receiver Detection Completed on 24
●	Console	OneView	12/18/2017 12:49:29 PM	—	[redacted]	[redacted]	Event	Automatic Trap Registration S...	Start Trap Receiver Detection on 87 Device
●	Console	OneView	12/18/2017 12:36:59 PM	—	[redacted]	[redacted]	Event	Automatic Syslog Registration...	Syslog Receiver Detection Completed on 2
●	Console	Resource	12/18/2017 12:35:47 PM	—	[redacted]	[redacted]	Event	Analytics Records	Analytics has resumed saving records, ser
●	Console	OneView	12/18/2017 12:35:10 PM	—	[redacted]	[redacted]	Event	Syslog Configuration Started	Start Syslog Configuration on 7 Devices X(
●	Console	Resource	12/18/2017 12:34:55 PM	—	[redacted]	[redacted]	Event	Historical Data	Historical data has resumed saving, server
●	Console	OneView	12/18/2017 12:34:39 PM	—	[redacted]	[redacted]	Event	Automatic Syslog Registration...	Start Syslog Receiver Detection on 87 Dev
●	Console	OneView	12/18/2017 12:34:29 PM	—	[redacted]	[redacted]	Event	Trap Configuration Started	Start Trap Receiver Configuration on 87 De
●	Console	Usage Dat...	12/18/2017 11:46:34 AM	—	[redacted]	[redacted]	Event	Usage Data Collection Failed ...	Inner Exception: A network-related or insta
●	Console	OneView	12/18/2017 11:02:03 AM	—	[redacted]	[redacted]	Event	Automatic Trap Registration C...	Trap Receiver Detection Completed on 24
●	Console	OneView	12/18/2017 11:01:13 AM	—	[redacted]	[redacted]	Event	Automatic Trap Registration S...	Start Trap Receiver Detection on 87 Device
●	Console	OneView	12/18/2017 10:48:44 AM	—	[redacted]	[redacted]	Event	Automatic Syslog Registration...	Syslog Receiver Detection Completed on 2
●	Console	Resource	12/18/2017 10:47:35 AM	—	[redacted]	[redacted]	Event	Analytics Records	Analytics has resumed saving records, ser
●	Console	OneView	12/18/2017 10:46:54 AM	—	[redacted]	[redacted]	Event	Syslog Configuration Started	Start Syslog Configuration on 7 Devices X(

Page 1 of 10 | Reset

Displaying 1 - 50 of 463

Last Updated: 12/18/2017 1:38:42 PM Uptime: 0 Days 20:11:14

Operations

Use the drop-down menu at the top of the table to filter events based on application:

- Selecting **Console** displays event logs with an **Event Type** of **Admin**, **Console**, and **Wireless**. Selecting Console View displays event logs with an **Event Type** of **Console** only.

  NOTE: Selecting both **Console** and **Console View** displays the event logs with an **Event Type** of **Console** twice.

- The Extreme Management Center event logs for Extreme Management Center and legacy components (Console, Inventory, Policy, NAC Manager, and Wireless) present the same data as the event logs in the actual applications.
- The Extreme Access Control Audit event log provides information on Extreme Access Control Registration events such as when a device or user is added during the registration process, or an end-system is added/removed/updated via the registration administration web page.
- The Extreme Access Control Engine event log displays engine events.

NOTE: Installed certificates using an MD5 RSA signature algorithm now generate an event in Extreme Management Center version 7.

The Wireless Audit event log allows you to view the configuration activity on Wireless Manager.

The Application Analytics event log displays Application Analytics engine events as well and Application Analytics configuration activity.

The Scheduler event log displays events for the scheduled tasks configured via the **Administration** tab. The event log includes task execution events and errors.

The Admin event log displays Extreme Management Center server and database administrative events, and Extreme Management Center user authentication and connection events. (In the legacy Console application, these events are included in the Console event log.)

You can manipulate the table data in several ways to customize the view for your own needs:

- Click the drop-down arrow to open the drop-down menu and select an application to include in the Events table.
- Click on the column headings to sort column data in ascending or descending order.

- Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
- Double-click on any row in the table to open a window that displays Event Details.

Event Log Column Definitions

Following are definitions of the Event Log table columns:

Severity — Indicates the potential impact of the event or trap. Hold the mouse pointer over a Severity icon to display a tool tip that provides the severity: Alert, Critical, Debug, Emergency, Error, Info, Notice, Warning. For traps, this column shows the Severity as defined in the `trapd.conf` file.

Event Type — Displays the application to which the event or trap is associated.

Category — Shows the category defined in the `trapd.conf` file for traps. For other events, it indicates the source of the information, either a Console Poller, local log, syslog, trap log, Error (java exceptions), etc.

Date/Time — Shows the date and time when an event or trap occurred.

Source — Shows the IP address of the host that was the source of the event or trap. If you want to display the source as a hostname (if available) you can set that option in the Suite-wide Alarm/Event Logs and Tables options.

Subcomponent — If the event or trap can identify a specific subcomponent of a device (or other source) which pinpoints the location of the problem, it is displayed here. One example of a subcomponent is an interface on a device.

Client — Displays the hostname of the source of the event.

User — The user that performed the action that triggered the event.

Type — Identifies the type of information for this row (event or trap).

Event — Shows the type of event or trap. For traps, this column shows the name of the event as defined in the `trapd.conf` file.

Information — Shows an summary explanation of the event or trap.

Buttons, Search Field, and Paging Toolbar

— The **Show Filters** button becomes active when any filters are applied. It opens a window that shows all active filters.

— The Search function allows you to search for full or partial matches on all fields. Enter the full or partial value you are searching for and click the **Search** button. Matching items are displayed in the table. Click the Reset button to clear the Search results and refresh the table.

— The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page. It also displays an indicator of the current and total number of pages. Enter a page number in the Page field and press Enter to quickly move to that page.

↻ — Refreshes the page.

— Clears the search field and search results, clears all filters, and refreshes the table.

Related Information

For information on related topics:

- Administration
- Network
- Reports
- Search
- Wireless

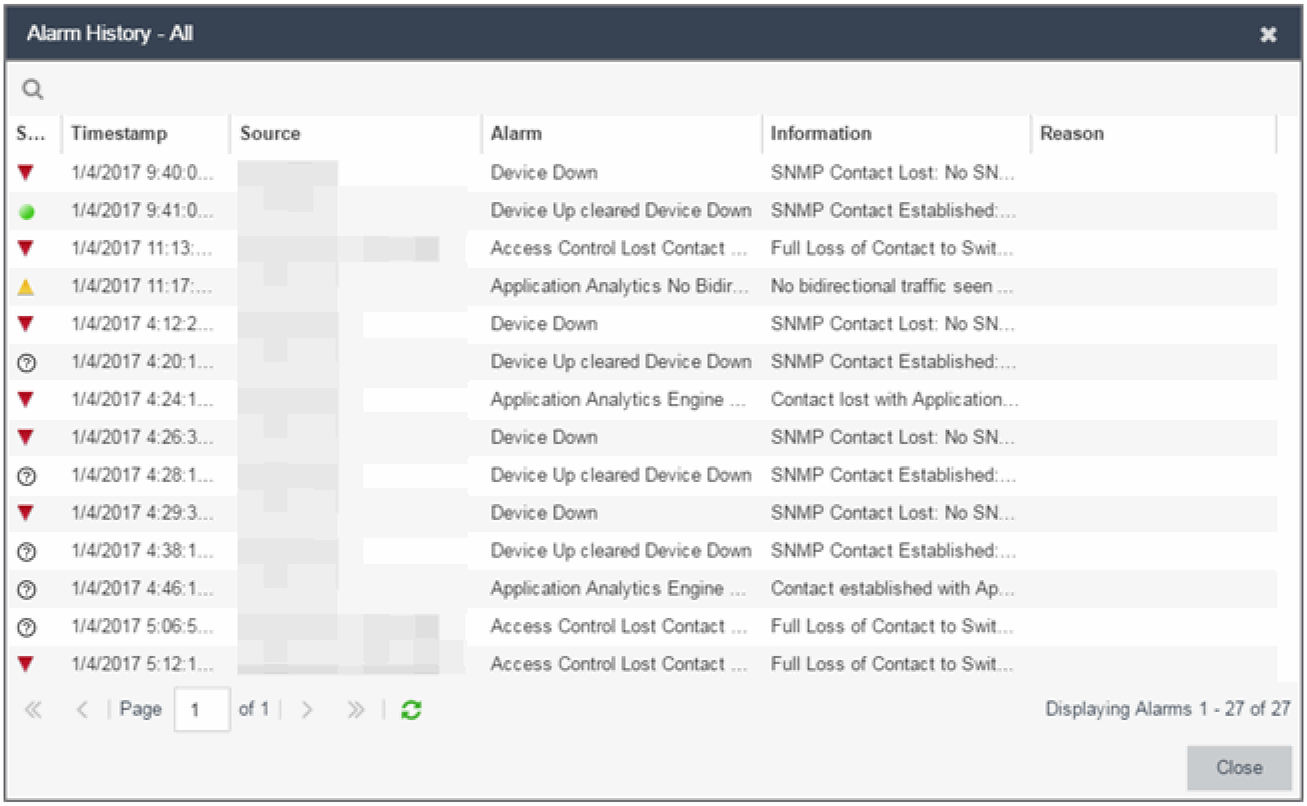
Alarm History

Extreme Management Center records alarm information whenever an alarm is raised and whenever an alarm is cleared, and displays the records in the Alarm History window, allowing you to view information about current and past alarms.

If a triggering event is stored with a selected history record, you can view the event by clicking the View Trigger button. If there is no triggering event, the button is disabled. You can enable an option to preserve alarm triggering events and store them with the alarm history record in the Alarm History section of the Alarm Options (**Administration** > **Options** > **Alarm**).

Use the following instructions to access the Alarm History window from the **Alarms** tab:

1. Select the alarm in the table for which you want to view the alarm history.
2. Click the **Menu** icon (≡).
3. Select the criteria by which the alarm history is displayed from the **Menu** drop-down menu:
    a. Select **Alarm History** > **All** to view the Alarm History for all devices.
    b. Select **Alarm History** > **By Source** to view an Alarm History for that device. If the Source includes a subcomponent (such as an interface on the device), then the alarm history is specific to that subcomponent.
    c. Select **Alarm History** > **By Alarm Name** to view an Alarm History for a specific alarm.



Alarm History - All

S...	Timestamp	Source	Alarm	Information	Reason
▼	1/4/2017 9:40:0...	[redacted]	Device Down	SNMP Contact Lost: No SN...	
●	1/4/2017 9:41:0...	[redacted]	Device Up cleared Device Down	SNMP Contact Established:...	
▼	1/4/2017 11:13:...	[redacted]	Access Control Lost Contact ...	Full Loss of Contact to Swit...	
▲	1/4/2017 11:17:...	[redacted]	Application Analytics No Bidir...	No bidirectional traffic seen ...	
▼	1/4/2017 4:12:2...	[redacted]	Device Down	SNMP Contact Lost: No SN...	
?	1/4/2017 4:20:1...	[redacted]	Device Up cleared Device Down	SNMP Contact Established:...	
▼	1/4/2017 4:24:1...	[redacted]	Application Analytics Engine ...	Contact lost with Application...	
▼	1/4/2017 4:26:3...	[redacted]	Device Down	SNMP Contact Lost: No SN...	
?	1/4/2017 4:28:1...	[redacted]	Device Up cleared Device Down	SNMP Contact Established:...	
▼	1/4/2017 4:29:3...	[redacted]	Device Down	SNMP Contact Lost: No SN...	
?	1/4/2017 4:38:1...	[redacted]	Device Up cleared Device Down	SNMP Contact Established:...	
?	1/4/2017 4:46:1...	[redacted]	Application Analytics Engine ...	Contact established with Ap...	
?	1/4/2017 5:06:5...	[redacted]	Access Control Lost Contact ...	Full Loss of Contact to Swit...	
▼	1/4/2017 5:12:1...	[redacted]	Access Control Lost Contact ...	Full Loss of Contact to Swit...	

Alarm Limits

To configure alarm action limits or an alarm (in the Actions tab of the **Alarm Configuration** window), right-click on an alarm history record and select **Alarm Limits** to open the **Alarm Tracking Information** window. This window displays the configured action limit, the number of times the action has been taken (Total Count), the number of times the action has been taken since the last reset, and the time of the next reset. You can also manually reset the alarm limit count using the **Reset Count** button. This resets the count for only this alarm on only this device or interface.

Alarm History Options

Change certain alarm history parameters in the Alarm History section of the Alarm options (**Administration** > **Options** > **Alarm**).

- By default, the alarm history is maintained for 14 days. You can change the number of days in the options.

- By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared. Select **Enable Detailed Alarm History** in **Administration** > **Options** > **Alarm** so that repeat occurrences of an alarm being raised are also recorded.
- You can enable an option to preserve alarm triggering events, so that any triggering events are stored with the alarm history record. If a triggering event is stored with the currently selected history record, you can view the event by clicking the View Trigger button in the Alarm History window. If there is no triggering event, the button is disabled.

Related Information

For information on related windows:

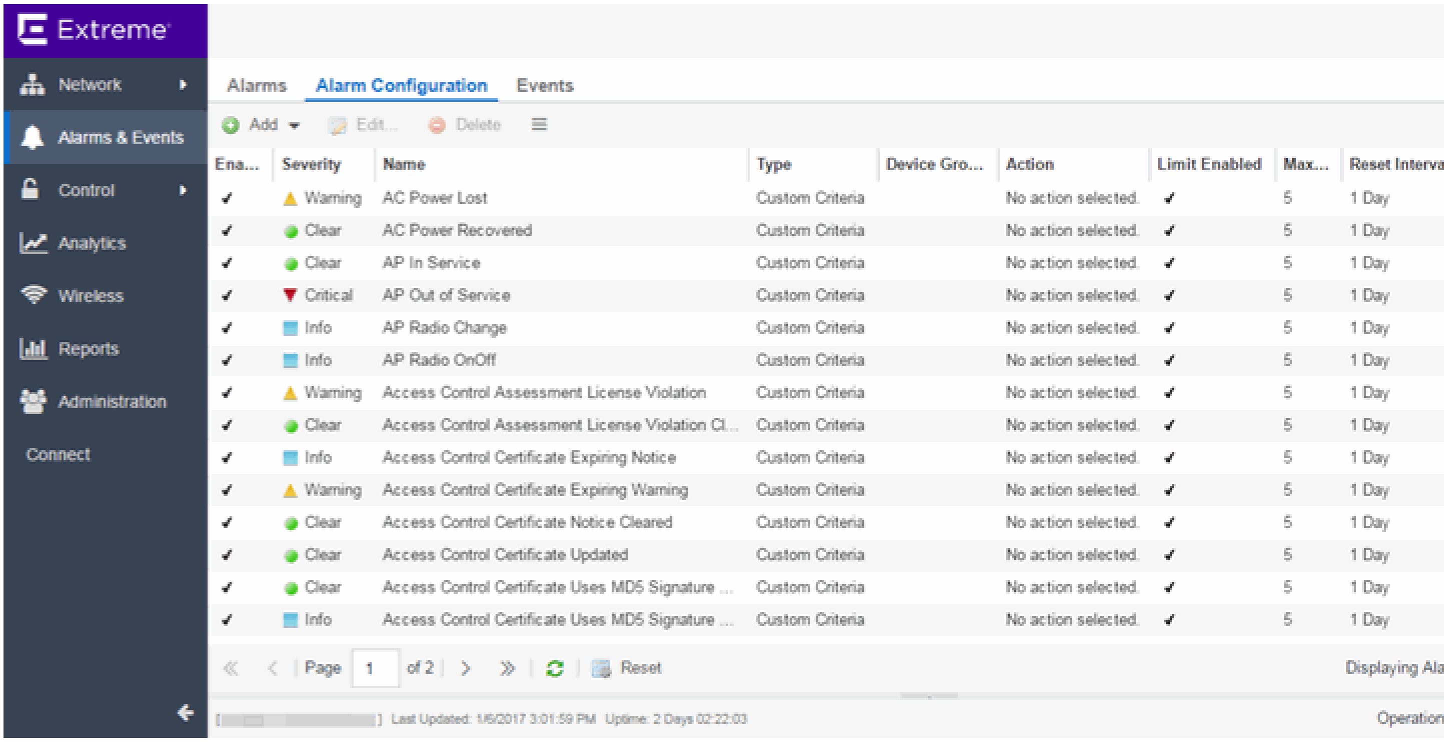
- Alarm Options

For information on related tasks:

- How to Configure Alarms

How to Configure Alarms

The **Alarm Configuration** tab lets you configure network alarms that provide status information for a particular problem or condition on a particular network device. Alarms are triggered when certain trap or event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed.



Ena...	Severity	Name	Type	Device Gro...	Action	Limit Enabled	Max...	Reset Interva
✓	▲ Warning	AC Power Lost	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	AC Power Recovered	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	AP In Service	Custom Criteria		No action selected.	✓	5	1 Day
✓	▼ Critical	AP Out of Service	Custom Criteria		No action selected.	✓	5	1 Day
✓	■ Info	AP Radio Change	Custom Criteria		No action selected.	✓	5	1 Day
✓	■ Info	AP Radio OnOff	Custom Criteria		No action selected.	✓	5	1 Day
✓	▲ Warning	Access Control Assessment License Violation	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	Access Control Assessment License Violation Cl...	Custom Criteria		No action selected.	✓	5	1 Day
✓	■ Info	Access Control Certificate Expiring Notice	Custom Criteria		No action selected.	✓	5	1 Day
✓	▲ Warning	Access Control Certificate Expiring Warning	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	Access Control Certificate Notice Cleared	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	Access Control Certificate Updated	Custom Criteria		No action selected.	✓	5	1 Day
✓	● Clear	Access Control Certificate Uses MD5 Signature ...	Custom Criteria		No action selected.	✓	5	1 Day
✓	■ Info	Access Control Certificate Uses MD5 Signature ...	Custom Criteria		No action selected.	✓	5	1 Day

Page 1 of 2 Reset Displaying Ala

Last Updated: 1/6/2017 3:01:59 PM Uptime: 2 Days 02:22:03 Operation

The alarm source, which is the device, interface, or AP that is the source of the trigger event, is considered to have an alarm until the alarm is cleared. You can view alarms and alarm status and clear alarms in the **Alarms & Events** > **Alarms** tab in Extreme Management Center. Using the **Alarm Configuration** tab, you can add a new alarm definition, which includes configuring the conditions (criteria) that triggers the alarm, and defining the actions performed to notify a person or network component about the problem, when the alarm is triggered.

You can create an alarm definition that detects a problem or condition and raises an alarm, and create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Device Down alarm is triggered when contact with a device is lost. Then, when contact is established with the device, the Device Up alarm automatically clears the Device Down alarm.

Extreme Management Center ships with a set of default alarm definitions, which you can see listed in the **Alarms** tab. You can use these default alarms as is, or enable, disable, delete or modify them, as desired.

This Help topic includes instructions for:

- Defining an Alarm
- Copying an Alarm
- Disabling Alarms
- Deleting Alarms
- Configuring Email Settings
- Resetting Alarm Action Limits
- Enabling/Disabling All
- Restoring Default Alarms
- Viewing Alarms
- Clearing Alarms

Defining an Alarm

You can use the **Alarm Configuration** tab to create new alarm definitions and define their criteria and actions, and to edit the criteria and actions for existing alarms.

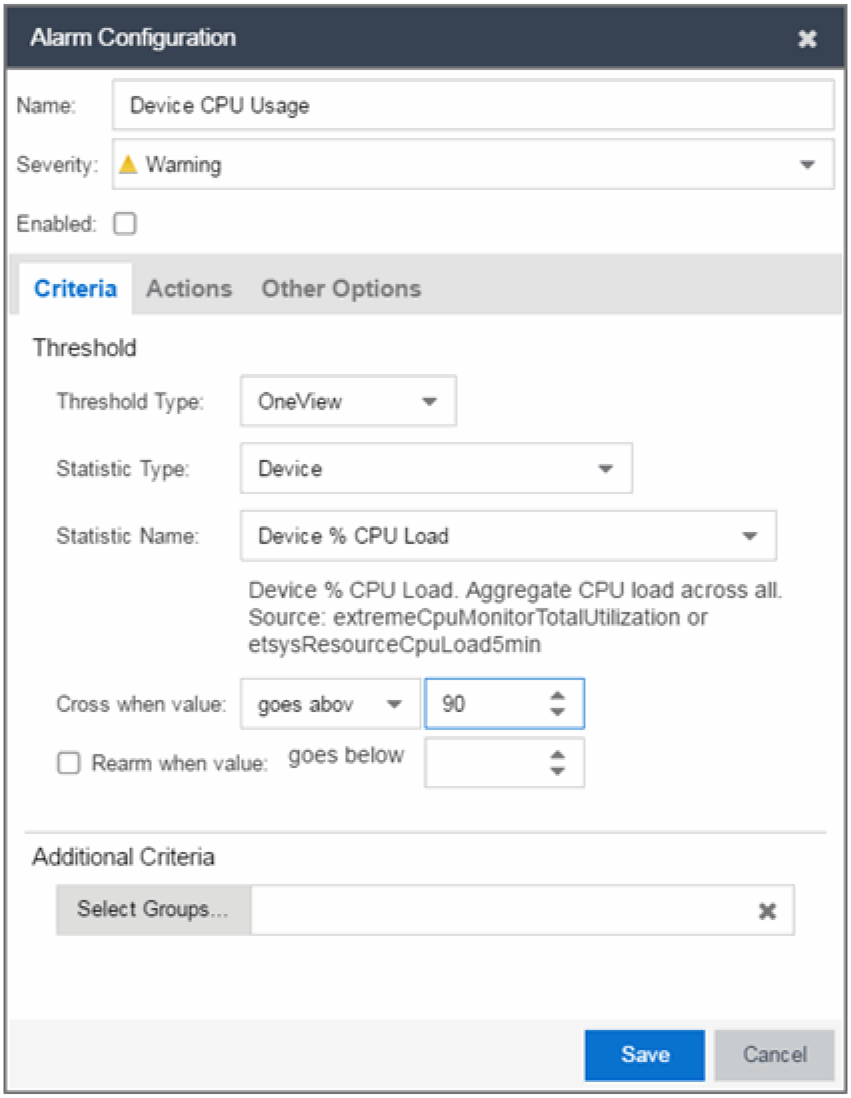
There are six types of alarms, each using different criteria to establish the alarm definition.

- **Selected Trap Alarm** — Triggers an alarm when a specific trap occurs. You are able to select from all the Trap IDs available for the devices modeled in the Extreme Management Center database.
- **Severity Alarm** — Triggers an alarm when an event or trap occurs to which you assign a specific level of severity. Select an event severity level (Emergency, Alert, Critical, Error, Warning, Notice, or Info) and whether the alarm is triggered by traps, or events, or both.

- **Status Change Alarm** — Triggers an alarm when the operational status for a device changes: **Contact Lost** triggers the alarm when contact with a device is lost, **Contact Established** triggers the alarm when contact is restored, and **Both** triggers the alarm when contact is lost and when contact is restored.
- **Flow Alarm** — Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. An alarm triggers when a flow matches criteria you configure.
- **Custom Criteria Alarm** — Triggers an alarm when very specific criteria you define is met.
- **Threshold Alarm** — Triggers the alarm when a specified value enters a defined range. For example, when CPU utilization exceeds 80% or when free disk space falls below 100 MB. There are two threshold alarm types: OneView and Application Analytics. This option is disabled if your Extreme Management Center license does not include Extreme Management Center features that support threshold alarms (such as device statistics collection) and you do not have an Application Analytics license.

To create a new alarm definition:

1. Click the **Add** button and select the type of Alarm you are creating from the drop-down menu. The **Alarm Configuration** window opens.



Alarm Configuration ✖

Name: Device CPU Usage

Severity: ▲ Warning

Enabled: □

Criteria | Actions | Other Options

Threshold

Threshold Type: OneView

Statistic Type: Device

Statistic Name: Device % CPU Load

Device % CPU Load. Aggregate CPU load across all. Source: extremeCpuMonitorTotalUtilization or etsysResourceCpuLoad5min

Cross when value: goes abov 90

□ Rearm when value: goes below

Additional Criteria

Select Groups... ✖

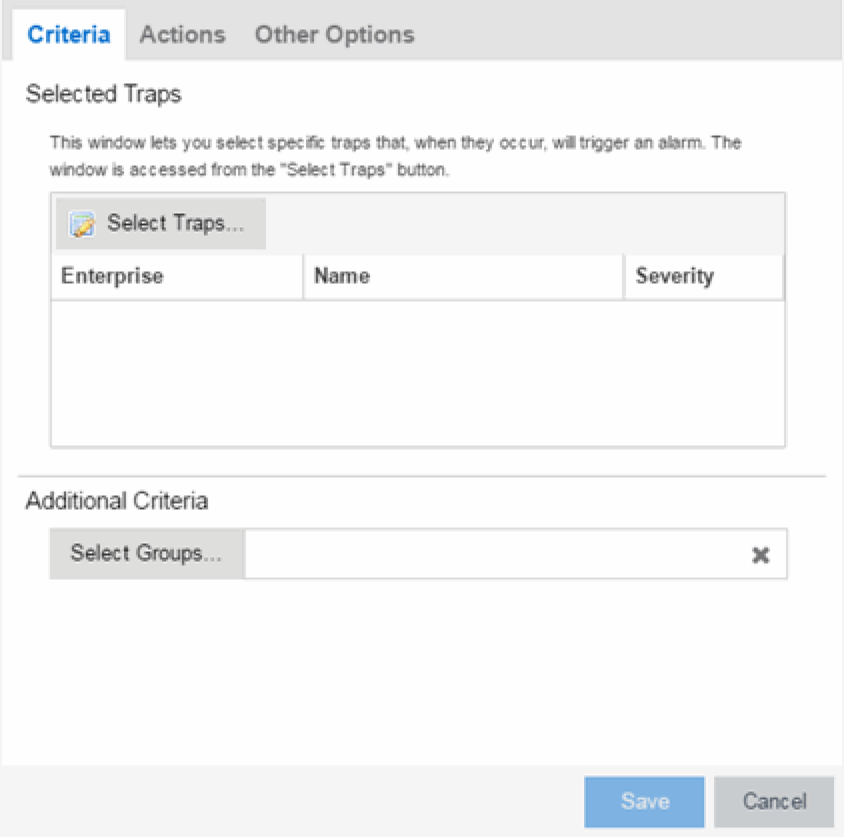
Save | Cancel

2. Enter a name for your new alarm definition in the **Name** field.
3. Select the appropriate severity level of the alarm definition in the **Severity** drop-down menu. The alarm can have its own specified severity regardless of the severity of the event or trap from which it is triggered.
   - ? (question mark) Set from Source — the alarm uses the severity level of the trigger event, for example a warning event.
   - ▼ (Red) Critical — A problem with significant implications.
   - ▶ (Orange) Error — A problem with limited implications.
   - ▲ (Yellow) Warning — A condition that might lead to a problem.
   - 🟦 (Blue) Info — Information only; not a problem.

- 🟢 (Green) Clear — An alarm that clears another alarm (for example, Device Up).

4. Select the **Enabled** checkbox to activate the alarm definition. You can disable an alarm definition to deactivate it without deleting the definition.
5. Enter the criteria that triggers the alarm. Options in the **Criteria** tab vary depending on the type of alarm you are creating.

- **Selected Trap Alarm**



Selected Traps

This window lets you select specific traps that, when they occur, will trigger an alarm. The window is accessed from the "Select Traps" button.

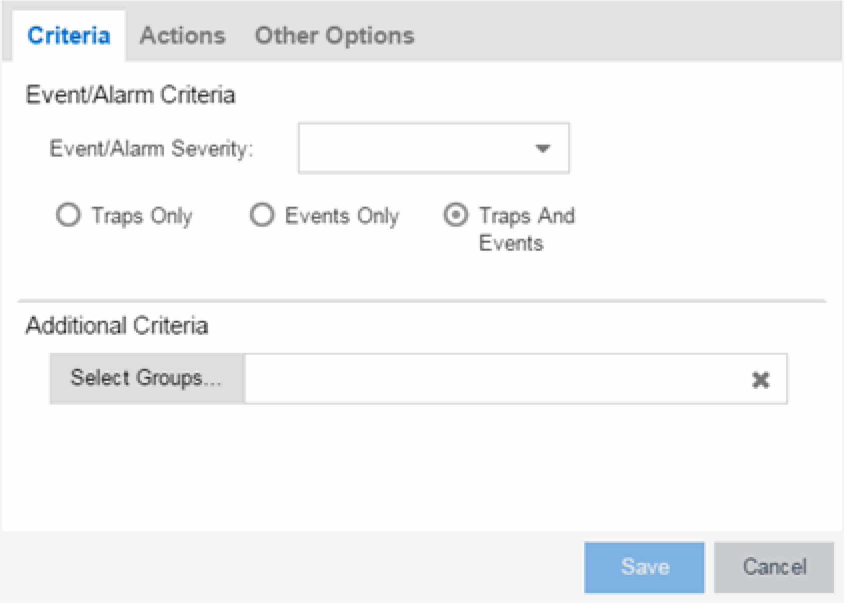
Enterprise	Name	Severity

Additional Criteria

a. Click the **Select Traps** button. The Select Traps window opens.
b. Select the traps that trigger the alarm.
c. Click **Save**.
d. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

e. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Severity Alarm



Event/Alarm Criteria

Event/Alarm Severity:

○ Traps Only ○ Events Only ● Traps And Events

Additional Criteria

Select Groups...

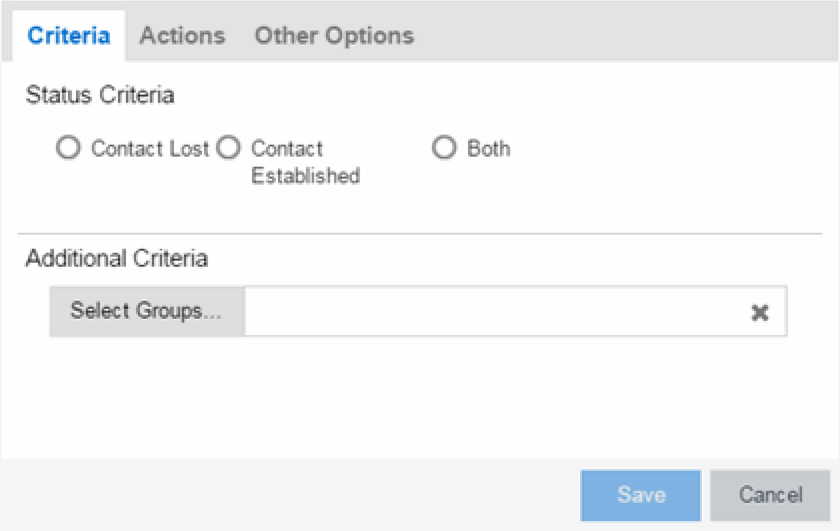
a. Select the severity of the event or trap required to generate the alarm from the drop-down menu (Emergency, Alert, Critical, Error, Warning, Notice, or Info). Traps or Events that occur and match the severity in this drop-down menu trigger the alarm. For example, you can create a severity alarm with an **Severity** of **Error** that is triggered when a trap or event occurs with an **Event/Alarm Severity** of **Alert**.

b. Select whether the alarm is triggered by traps, or events, or both.

c. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

d. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Status Change Alarm

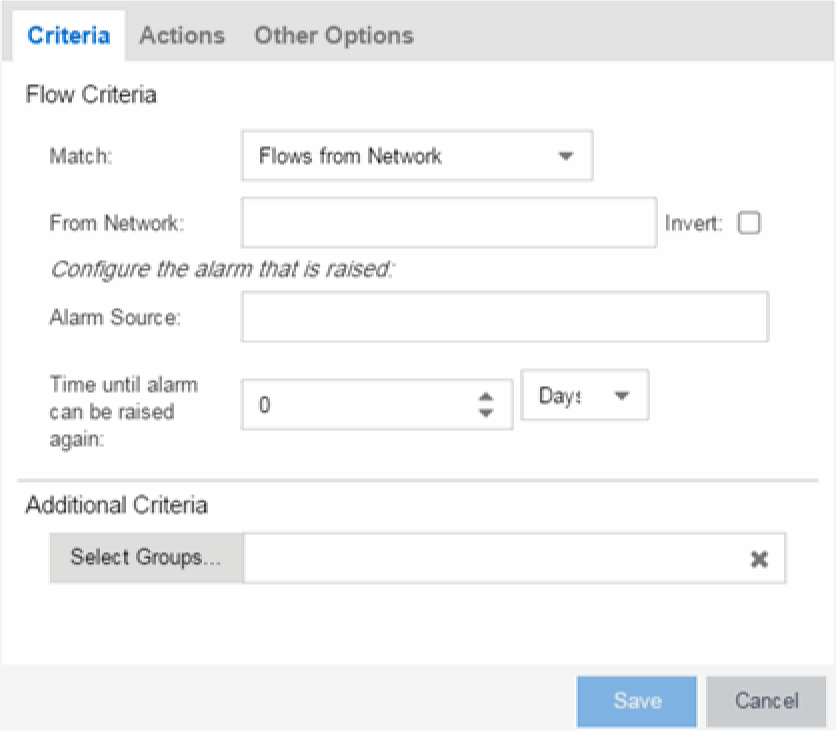


a. Select whether the alarm triggers when contact with a device is lost (Contact Lost), restored (**Contact Established**), or when contact is lost and when contact is regained (**Both**).

b. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

c. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Flow Alarm



Flow Criteria

Match: Flows from Network

From Network: Invert: □

Configure the alarm that is raised:

Alarm Source:

Time until alarm can be raised again: 0 Days

Additional Criteria

Select Groups...

a. Select how the flow is matched to trigger a flow alarm in the **Match** drop-down menu. Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. NetFlow is a flow-based data collection protocol that provides information about the packet flows being sent over a network. K-Series, S-Series, and N-Series devices support NetFlow flow collection.

   - **Flows from Network** — Match a flow's source IP address to the specified network.
   - **Flows to Network** — Match a flow's destination IP address to the specified network.
   - **Flows from Network from Port** — Match a flow's source IP address and port number to the specified network and port.
   - **Flows from Port to Network** — Match a flow's source port number and destination IP address to the specified port and network.

  - **Flows from Network with low TTL** — Match a flow's source IP address and TTL value to the specified network and the **TTL at or below** value.

b. Enter the **Network** or **Port** monitored by the flow alarm

  - **From/To Network** — A network is identified as a set of IP masks. The mask is used as a filter to define a range of IP addresses. Masks can be entered in CIDR or dotted-decimal format.
    - **CIDR** — CIDR format uses a slash followed by a number between 8 and 32, to define the number of contiguous, left-most "one" bits that define the network mask. For example, */16* indicates a 16-bit mask. Here is an example of a From/To Network value using the CIDR format: 10.20.0.0/16,10.20.0.0/24
    - **Dotted-Decimal** — Dotted decimal format represents network masks as four octets separated by periods. For example, a 16-bit mask in dotted decimal notation is *255.255.0.0*. Here is an example of a From/To Network value using the dotted-decimal format: 10.20.0.0/255.255.0.0,10.20.88.0/255.255.255.0
    - For example, if you entered either 10.20.0.0/16 (CIDR) or 10.20.0.0/255.255.0.0 (Dotted-Decimal) in the From/To Network field, then all incoming packets in the range 10.20.00.00 through 10.20.255.255 would result in an address match.
  - **From Port** — Enter the port number to be matched.
  - **TTL at or below** — Enter a value that triggers an alarm when the TTL value in the packet's TTL field is equal to or less than the value entered.
  - Select the **Invert** checkbox if you want the flow criteria to trigger the alarm when it does **not** match the specified values.

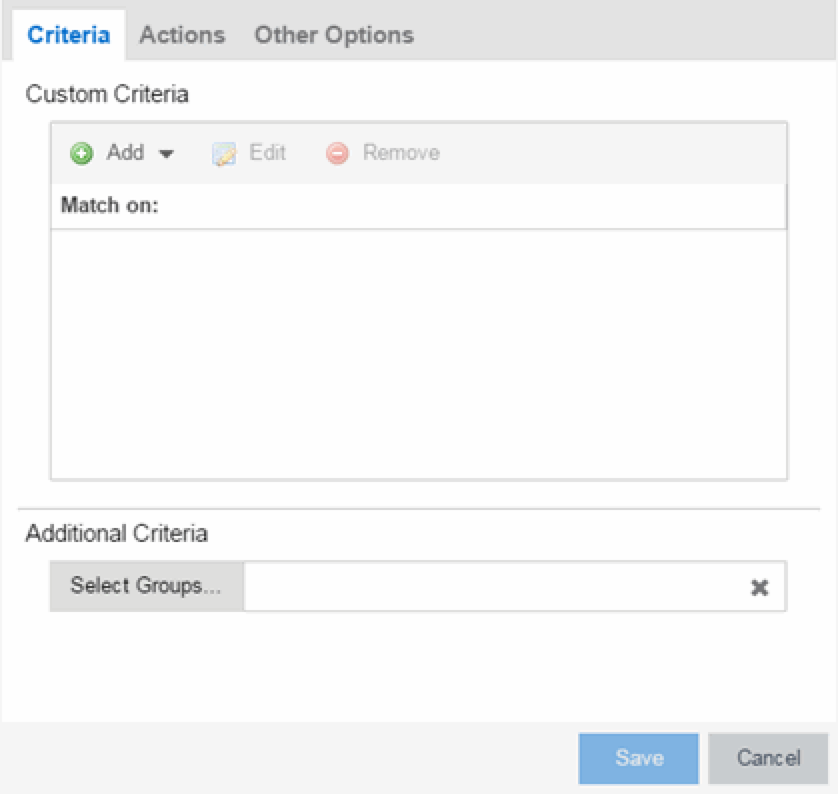
c. Enter a phrase in the **Alarm Source** field used as the source of the alarm.

d. Enter the amount of time, in minutes, hours, or days that must pass until the alarm can trigger again in the **Time until alarm can be raised again** field. This prevents a large number of alarms being triggered, if many flows match the alarm criteria. If you select **Never**, the alarm only triggers one time. Once you manually clear the alarm, it can be triggered again.

e. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

f. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to [Step 6 for information about configuring rule actions](#).

- Custom Criteria Alarm



a. Click the **Add** drop-down menu and select the criteria by which the alarm triggers.

  - **Severity Criteria** — Select one or more severity levels against which to match.

    - **Match Selected** — The reported Severity is matched against any of the Severity levels selected in the list.

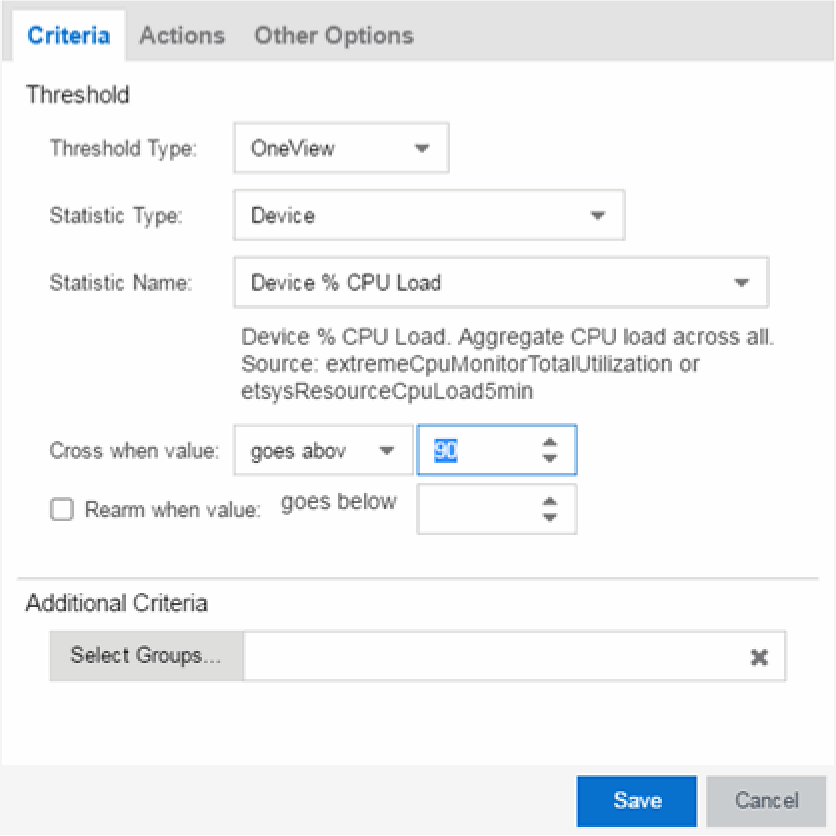
    - **Exclude Selected** — The reported Severity matches if it is not one of the Severity levels selected in the list.
- **Category Criteria** — Select one or more event categories to match against the Category column of the event. An event category is a way to group related events. For example, all events related to device discovery would be in the "Discover" category
    - **Match Selected** — The reported Category is matched against any of the categories selected in the list.
    - **Exclude Selected** — The reported Category matches if it is not one of the categories selected in the list.
- **Type Criteria** — Select one or more message types (Event, Inform, Trap) to match against the Type column of the event.
    - **Match Selected** — The reported Type is matched against any of the types selected in the list.
    - **Exclude Selected** — The reported Type matches if it is not one of the message types selected in the list.
- **Event Criteria** — Select one or more event types to match against the Event column of the event.
    - **Match Selected** — The reported Event is matched against any of the event types selected in the list.
    - **Exclude Selected** — The reported Event matches if it is not one of the event types selected in the list.
- **Host or IP Criteria** — Select one or more host names or IP/Subnet addresses to match against the value of the address appearing in the Source column of the event. The list of host names and IP/Subnet addresses can be edited by clicking the **Edit List** button.
    - **Match Selected** — The reported host name or IP/Subnet address is matched against any of the host or IP/Subnets selected in the list.
    - **Exclude Selected** — The reported host name or IP/Subnet address matches if it is not one of the host or IP/Subnets selected in the list.
- **Log Criteria** — Select one or more Event Logs against which to match.

        - **Match Selected** — The log where the event was received is matched against any of the logs selected in the list.
        - **Exclude Selected** — The log where the event was received matches if it is not one of the logs selected in the list.
    - **Phrase Criteria** — Select one or more text strings (phrases) to match against text in the Information column of the event or trap. The list of text phrases can be edited by clicking the **Edit List** button.
        - **Match Selected** — The information text string is matched against one or more phrase selected from the list.
        - **Exclude Selected** — The information text string matches if it is not one of the phrases selected from the list.

b. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

c. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Threshold Alarm



Threshold

Threshold Type: OneView

Statistic Type: Device

Statistic Name: Device % CPU Load

Device % CPU Load. Aggregate CPU load across all. Source: extremeCpuMonitorTotalUtilization or etsysResourceCpuLoad5min

Cross when value: goes abov 90

□ Rearm when value: goes below

Additional Criteria

Select Groups...

a. Select a **Threshold Type**.

   - **OneView** — The Extreme Management Center (formerly OneView) Collector gathers historical reporting data over time, which is then used in Extreme Management Center reports. Threshold alarms are raised when the reporting data matches a threshold alarm criteria.
   - **Application Analytics** — The Application Analytics engine generates Application Analytics threshold alarms as part of the application usage collection process. Threshold alarms are raised when hourly or high-rate usage data matches a threshold alarm criteria. Each target record produced on the Application Analytics engine is evaluated at the end of each collection interval to see if it matches alarm criteria. If a statistic has crossed a configured threshold, an alarm in raised. Alarms can track single target types as well as target combinations. They can reference specific targets, for example a specific application such as Facebook, or they can

reference all the targets in a target type, for example all applications. Only the target types and target combinations that are collected by Application Analytics can be used in alarms.

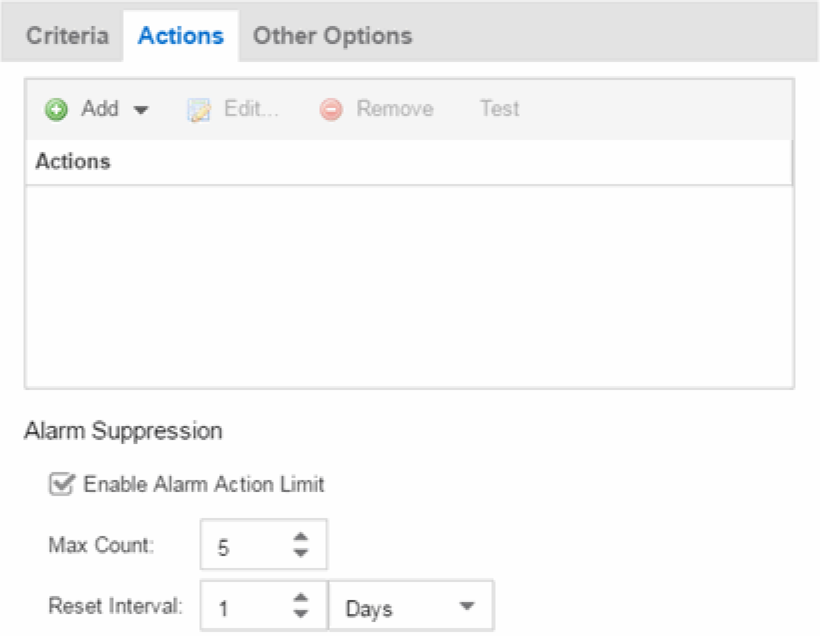
b. Select the criteria against which the threshold is compared.

c. Enter the threshold value. When the value crosses the established threshold for the criteria you select, the alarm triggers.

d. Click **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and click **OK**. Not selecting any device groups means the alarm applies to all devices.

e. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to [Step 6 for information about configuring rule actions]().

6. Click the **Add** drop-down menu to select the actions performed when the alarm is triggered.



☑ Enable Alarm Action Limit

Max Count: 5

Reset Interval: 1 Days

- **Add Email Action** — Sends an email when the alarm is triggered. Use the **Destination** drop-down menu to select one of your pre-defined email lists. Extreme Management Center comes preloaded with a default email list called Helpdesk. You can rename this list, but it cannot be deleted. Click the **Edit Email Lists** button to define a new list. (You must have your SMTP E-Mail

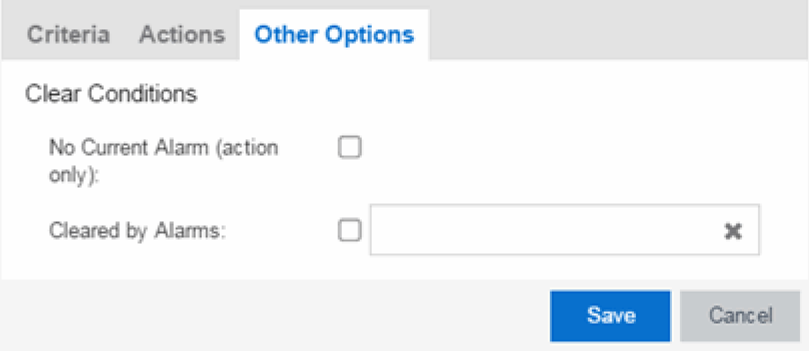
Server options configured.) There are default formats for the subject and body of the email you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by clicking **Show Keywords**. Click the **Save** button to save the email action to the list of actions for the alarm definition.

- **Add Syslog Action** — Creates a syslog message when the alarm is triggered. Enter the IP address or hostname that identifies the syslog server where the message is sent. There is a default format for the syslog message sent to the server you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by clicking **Show Keywords**. Click the **Save** button to save the syslog action to the list of actions for the alarm definition.
- **Add Trap Action** — Sends an SNMP trap when the alarm is triggered. Enter the IP address for a trap receiver where the trap is sent in the **Trap Server** field. Valid trap receivers are systems running an SNMP Trap Service. From the **Credential** drop-down menu, select the appropriate SNMP credential to use when sending the trap to the trap receiver. Credentials are defined in the **Profiles/Credentials** tab in the Authorization/Device Access window (Tools > Authorization/Device Access). There is a default format for the trap message you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by clicking **Show Keywords**. Click the **Save** button to save the trap action to the list of actions for the alarm definition.
- **Add Custom Action** — Runs a custom program or script on the Extreme Management Center Server when the alarm is triggered. In the **Program** field, enter the name of the program. In the **Working Directory** field, enter the path to the directory from which the program is executed. Any path references within your program that are not absolute paths, are relative to the working directory. There is a default set of arguments passed to the program you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by clicking **Show Keywords**. Click the **Save** button to save the email action to the list of actions for the alarm definition.
- If you want to set a limit on the number of times the system performs the alarm action for this alarm, check **Enable Alarm Action Limit** and type a number into the **Max Count** field. Once the limit is reached, the alarm is still recorded, but no further actions are performed. If you have configured multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. Each alarm source has its own action count for an alarm, so when the **Max Count** limit is reached for one alarm source, actions may still occur for other alarms from that alarm source as well as for other

alarm sources. If **Save** is not checked, there is no limit placed on the number of times the action is performed.

- You can specify a **Reset Interval**, which automatically resets the action count after the time limit specified, allowing actions to resume for that alarm source. If the reset interval is set to **None**, then once the alarm limit is reached, the alarm does not reset unless manually reset.
- You can test an alarm action by clicking the **Test** button. (You must save an alarm before you can test it.) You can also override the action.

7. In the **Other Options** subtab, select how you want to clear the alarm.

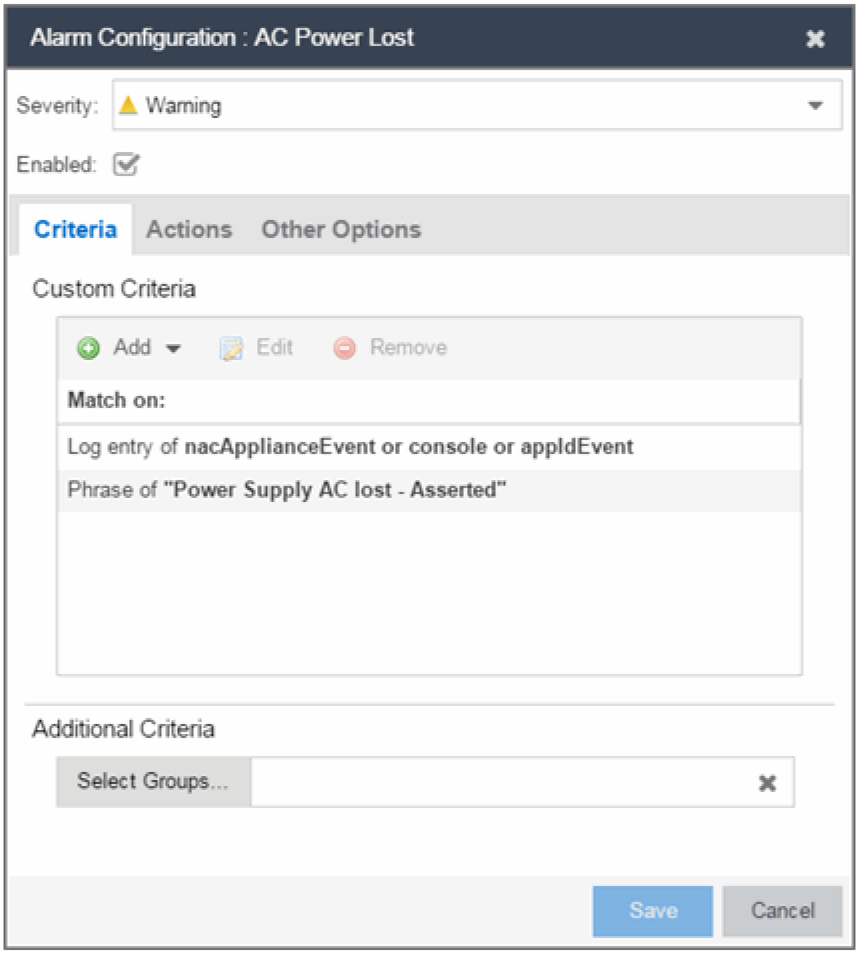


- **No Current Alarm (action only)** — When this option is selected, the trigger event causes the system to perform the configured actions, but does not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source does not change, and no alarm is added to the system.
- **Cleared by Alarm** — This option allows you to select the alarm(s) used to clear the alarm you are defining. You must first create the alarm definitions for the clearing alarms, which must have the alarm severity set to "Clear". The clearing alarms are triggered when the problem or condition is removed. Then, use the **Select Alarms** button to open a window to select one or more clearing alarms that clear the alarm you are defining.

8. Click **Save** to create the alarm and close the Alarm Configuration window.

To modify an existing alarm:

1. In the Alarm Configurations view, select the alarm definition you want to change.
2. Double-click the Alarm Definition. You can also click the **Edit** button or right-click the alarm definition, and select **Edit**. The Alarm Configuration window opens.



Alarm Configuration : AC Power Lost

Severity: Warning

Enabled: ☑

Custom Criteria

Match on:

Log entry of **nacApplianceEvent or console or appIdEvent**

Phrase of **"Power Supply AC lost - Asserted"**

Additional Criteria

3. Edit the necessary fields. For additional information, see [To create a new alarm definition]().
4. Click **Save** to edit the alarm definition and close the Alarm Configuration window.

Copying an Alarm

You can also copy and modify existing alarm definitions using the **Alarm Configuration**. This provides you with a template from which to configure a new alarm.

To copy an alarm, right-click the alarm and select **Copy** to open the Copy Alarm Definition window. Enter a unique name for the new alarm and click **OK**. You can then [edit the alarm]() to the desired configuration.

Disabling Alarms

There may be times when you want to disable an alarm definition without deleting it. For example, you might want to temporarily disable a Device Down alarm definition while you are performing maintenance on that device.

To disable an alarm, open the Alarm Configuration view, right-click the alarm you want to disable, and select **Disable**.

Deleting Alarms

To completely remove an alarm definition you no longer use, you can delete the alarm definition from Extreme Management Center.

To delete an alarm, open the Alarm Configuration view, select the alarm definition you want to delete, and click the **Delete** button.

Configuring Email Settings

From the **Alarm Configuration** tab, you can configure or edit the email address to which alarm information is sent for an alarm definition when the alarm is triggered.

To configure the email address to which alarm information is sent, open the **Alarm Configuration** tab, select the alarm definition for which you want to configure or change the email settings, click the **Menu** icon (≡) or right-click the alarm definition and select the **Edit** button. Email actions are configured on the **Actions** tab of the **Alarm Configuration** window.

Resetting Alarm Action Limits

Once an action limit is reached for an alarm, the action no longer occurs when an alarm triggers. From the **Alarm Configuration** tab, you can reset the action limits for your alarms so the actions occur when an alarm is triggered.

To reset the action limits, open the **Alarm Configuration** tab, select the alarm definition for which you want to reset the action limits, click the **Menu** icon (≡) or right-click the alarm definition and select **Reset Alarm Action Limits**.

Enabling/Disabling All

From the **Alarm Configuration** tab, you can enable or disable all of your alarms at once.

To enable or disable all of your alarms, open the **Alarm Configuration** tab, click the **Menu** icon (≡), and select **Enable All** or **Disable All**, respectively.

Restoring Default Alarms

From the **Alarm Configuration** tab, you can restore the default alarms that you delete or modify.

To restore the default alarms, open the **Alarm Configuration** tab, click the **Menu** icon (≡), and select **Restore Default Alarms**.

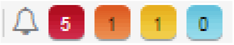
NOTE: The time required to restore default alarms can vary. When the process is complete, you are notified by a confirmation window.

Viewing Alarms

You can view device/alarm status in multiple places throughout Extreme Management Center.

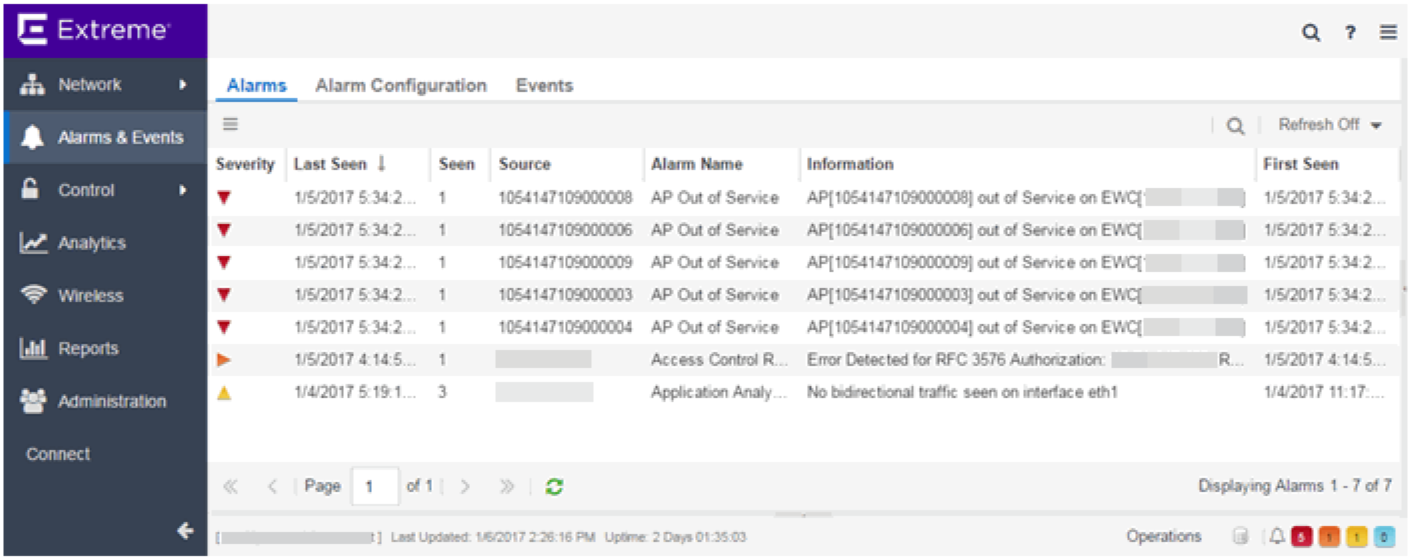
Extreme Management Center

Every Extreme Management Center page includes a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) that is present in the entire system. If there are no current alarms, the status displays all zeroes. Click on an indicator to open the **Alarms** tab filtered to display the alarms of that severity.



Alarms & Events Tab

You can view current alarm information in the **Alarms & Events** > **Alarms** tab. Use the configuration menu button or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason you cleared the alarm, which is recorded in the Alarm History.



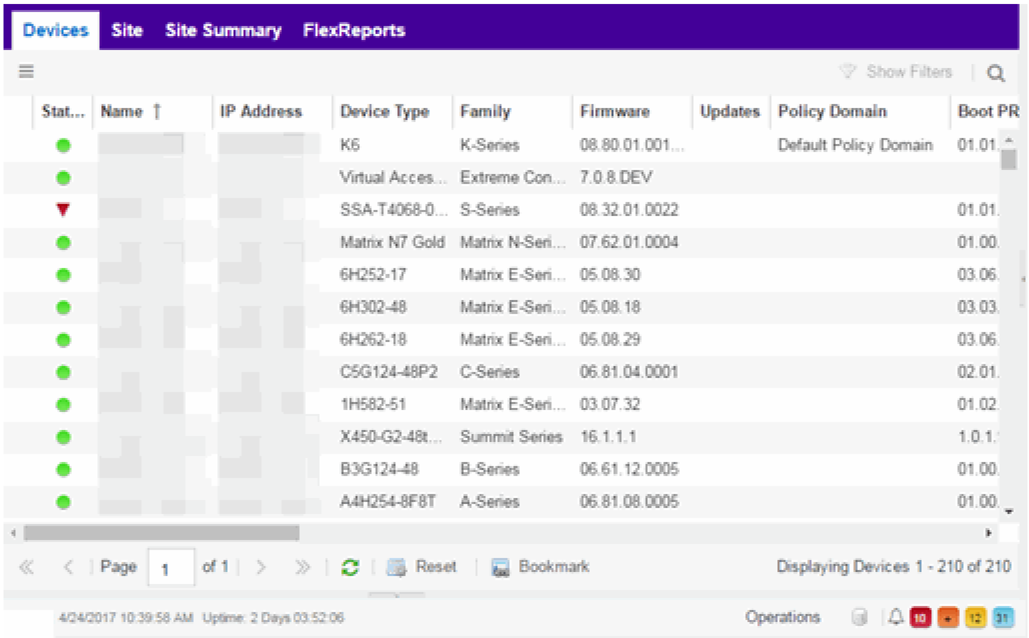
Severity	Last Seen	Seen	Source	Alarm Name	Information	First Seen
▼	1/5/2017 5:34:2...	1	1054147109000008	AP Out of Service	AP[1054147109000008] out of Service on EWC[[redacted]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000006	AP Out of Service	AP[1054147109000006] out of Service on EWC[[redacted]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000009	AP Out of Service	AP[1054147109000009] out of Service on EWC[[redacted]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000003	AP Out of Service	AP[1054147109000003] out of Service on EWC[[redacted]	1/5/2017 5:34:2...
▼	1/5/2017 5:34:2...	1	1054147109000004	AP Out of Service	AP[1054147109000004] out of Service on EWC[[redacted]	1/5/2017 5:34:2...
▶	1/5/2017 4:14:5...	1	[redacted]	Access Control R...	Error Detected for RFC 3576 Authorization: [redacted] R...	1/5/2017 4:14:5...
▲	1/4/2017 5:19:1...	3	[redacted]	Application Analy...	No bidirectional traffic seen on interface eth1	1/4/2017 11:17:...

Displaying Alarms 1 - 7 of 7

[[redacted]] Last Updated: 1/6/2017 2:26:16 PM Uptime: 2 Days 01:35:03

Network Tab

You can view the alarm status for a device in the **Status** column from within the My Network navigation tree on the **Network** tab. The colored circle indicates the severity of the most severe alarm on the device. A green icon indicates that there are no alarms and the device is up. A red icon indicates a critical alarm or the device is down. Double-click on the **Status** icon to open a new page with detailed information about the alarms for that device. For additional information, see Network tab help topic.

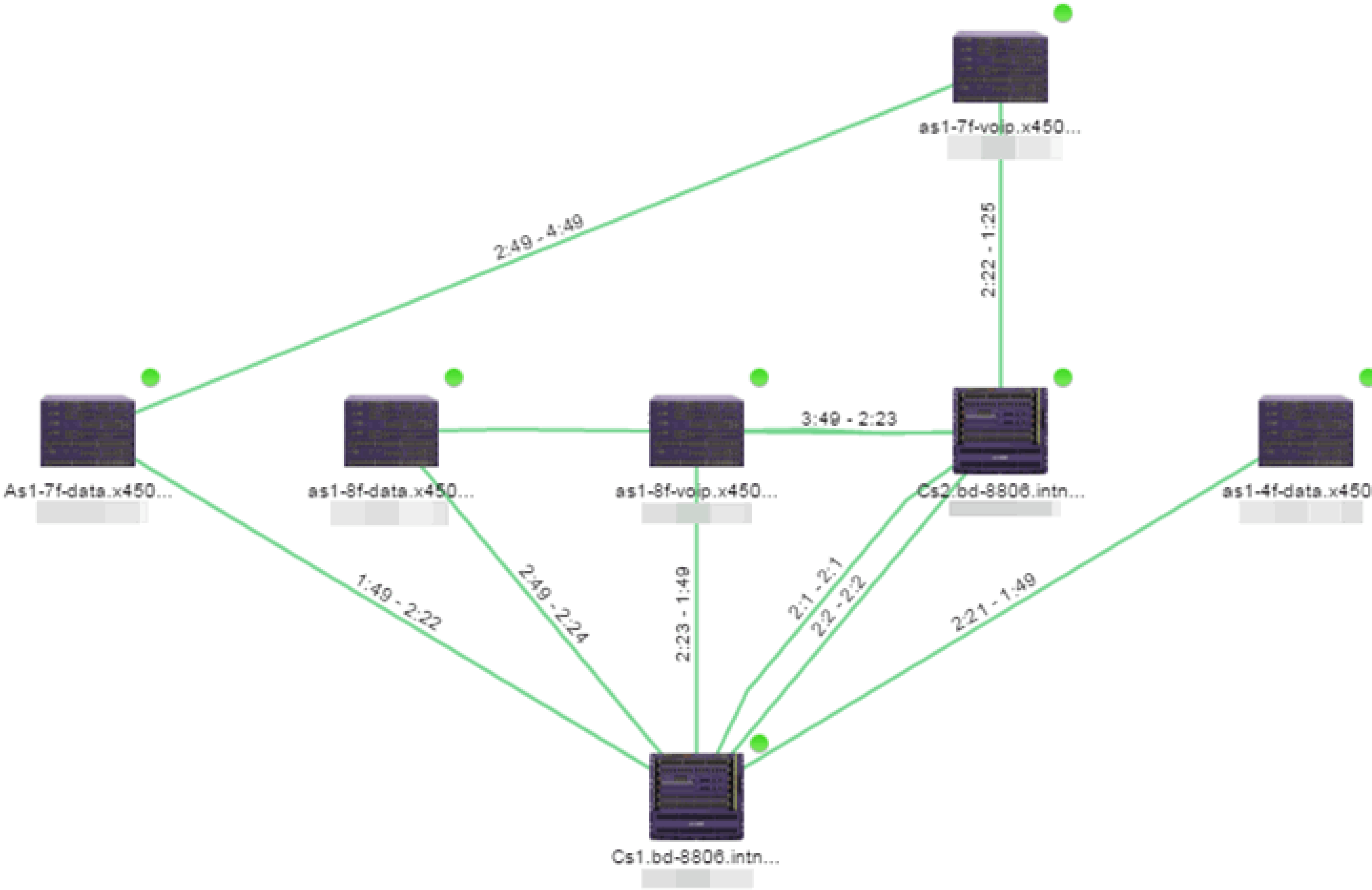


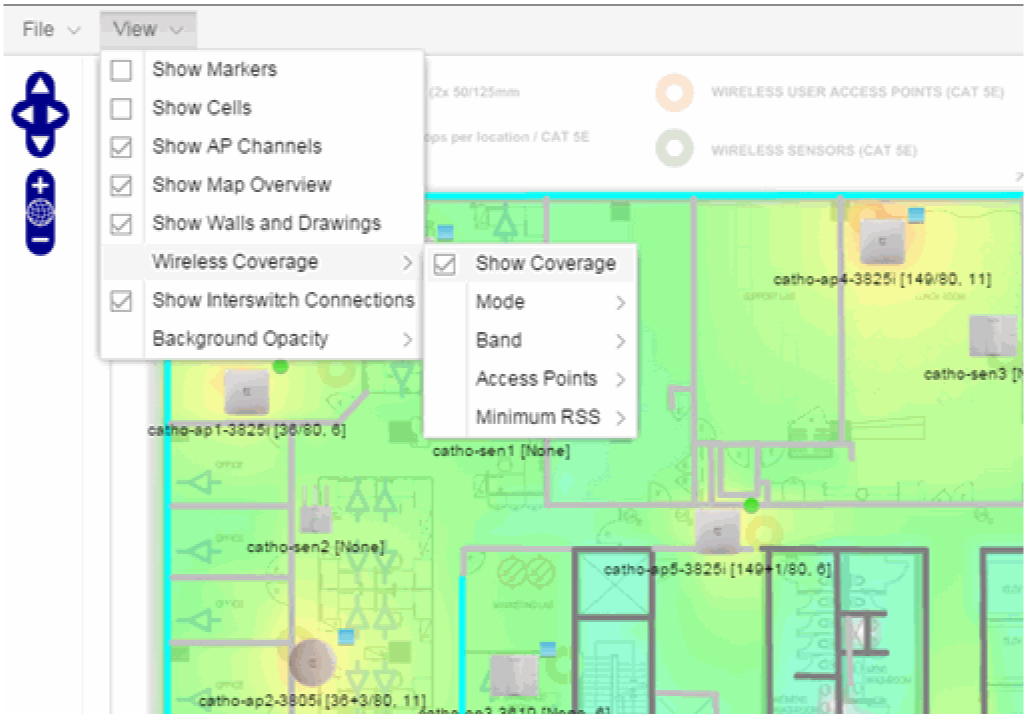
Stat...	Name ↑	IP Address	Device Type	Family	Firmware	Updates	Policy Domain	Boot PR
●	[redacted]	[redacted]	K6	K-Series	08.80.01.001...		Default Policy Domain	01.01.
●	[redacted]	[redacted]	Virtual Acces...	Extreme Con...	7.0.8.DEV			
▼	[redacted]	[redacted]	SSA-T4068-0...	S-Series	08.32.01.0022			01.01.
●	[redacted]	[redacted]	Matrix N7 Gold	Matrix N-Seri...	07.62.01.0004			01.00.
●	[redacted]	[redacted]	6H252-17	Matrix E-Seri...	05.08.30			03.06.
●	[redacted]	[redacted]	6H302-48	Matrix E-Seri...	05.08.18			03.03.
●	[redacted]	[redacted]	6H262-18	Matrix E-Seri...	05.08.29			03.06.
●	[redacted]	[redacted]	C5G124-48P2	C-Series	06.81.04.0001			02.01.
●	[redacted]	[redacted]	1H582-51	Matrix E-Seri...	03.07.32			01.02.
●	[redacted]	[redacted]	X450-G2-48t...	Summit Series	16.1.1.1			1.0.1.
●	[redacted]	[redacted]	B3G124-48	B-Series	06.61.12.0005			01.00.
●	[redacted]	[redacted]	A4H254-8F8T	A-Series	06.81.08.0005			01.00.

Displaying Devices 1 - 210 of 210

4/24/2017 10:39:58 AM Uptime: 2 Days 03:52:06

You can also view the alarm status for a device in device maps, found in the World map navigation tree. Topology and geographic maps show the status of devices in your network and floor plans show the status of wireless access points. As with devices in the My Network navigation tree, the colored circle associated with a device or access point in a map indicates the severity of the most severe alarm on the device. For additional information, see View and Search Maps.


as1-7f-voip.x450...
2:49 - 4:49
2:22 - 1:25
As1-7f-data.x450...
as1-8f-data.x450...
as1-8f-voip.x450...
3:49 - 2:23
Cs2.bd-8806.intn...
as1-4f-data.x450
1:49 - 2:22
2:49 - 2:24
2:23 - 1:49
2:1 - 2:1
2:2 - 2:2
2:21 - 1:49
Cs1.bd-8806.intn...


File
View
☐ Show Markers
☐ Show Cells
☑ Show AP Channels
☑ Show Map Overview
☑ Show Walls and Drawings
Wireless Coverage >
☑ Show Interswitch Connections
Background Opacity >
☑ Show Coverage
Mode >
Band >
Access Points >
Minimum RSS >
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
catho-ap4-3825i [149/80, 11]
catho-sen3
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap2-3805i [36+3/80, 11]

Clearing Alarms

An alarm can be cleared manually or automatically.

To clear an alarm manually:

In the **Alarms & Events** > **Alarms** tab, **Menu** icon (≡) in the upper left corner or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason that the alarm was cleared, which is recorded in the Alarm History.

To clear an alarm automatically:

An alarm is cleared automatically by another alarm called a "Clearing Alarm". For example, you can create a Device Up alarm so that when contact is established with a device, the alarm automatically clears a Device Down alarm.

Clearing Alarms are configured in the Alarm Configuration window with an **Alarm Severity** set to **Clear**. The alarm is defined so that when it is triggered, it removes an alarm rather than adds one.

In addition, a threshold alarm can be configured to "self-clear". For additional information, see How to Clear Threshold Alarms in Extreme Management Center.

This is called re-arming the alarm. Re-arming allows the threshold alarm to clear itself when the monitored statistic is restored to an acceptable range, without requiring a clearing alarm. When an alarm self-clears, no action is triggered.

Related Information

For information on related concepts:

- Alarms & Events

For information on related tasks:

- How to Configure Alarms in Alarms Manager

Wireless

The **Wireless** tab in Extreme Management Center provides dashboards, Top N information, and detailed charts to help you monitor the overall status of your wireless network. Reports are flexible and interactive, allowing you to configure time ranges and data rollup values to use for each report. Use the report Search and Filter capabilities to narrow down the data shown in the report tables. Click on links in the reports to quickly drill down to more detailed information.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

To view wireless reporting data, you must enable statistics collection for your wireless controller devices from either **Network** tab (or the legacy Console application in the device tree or **Device Properties** tab). On the **Network** tab, right-click on a wireless controller and select **Device** > **Collect Device Statistics**. In the Console device tree or **Device Properties** tab, right-click the controller and select the OneView > **Collect Device Statistics** checkbox. When you enable Wireless Controller statistics collection (which includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics), you also have the option to collect wireless client statistics. Extreme Management Center begins collecting data on the controller device it uses in its Wireless reports.

To view all Wireless reports, you must be a member of an authorization group that has been assigned full read access capabilities to all of the Extreme Management Center tabs and reports. For more information on authorization capabilities, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Suite-Wide Tools > Authorization Device Access.

This Help topic provides information on each Wireless report, plus a section on helpful report features and functionality.

- Dashboard
- Controllers
- Access Points
- Clients

- Threats
- Reports

Dashboard

The Dashboard menu in the upper left corner provides access to the Dashboard report and the Overview report, as well as additional Top N and summary reports on your wireless devices and clients.

Overview Report

The Overview displays a selection of reports that provide highly summarized information about your wireless network. Click the **Gear** button (⚙) to open additional fields from which you can configure the information presented in the reports.

Click on links to drill down for more information. Use the drop-down menus to select the date, time, and whether to display Daily, Hourly, or Raw Data.

Wireless Network Summary Report

The Wireless Network Summary dashboard displays three reports displaying the wireless client information, wireless and wired bandwidth usage, and the number of active APs in your network.

Use the drop-down menus to select the time displayed and whether to display Daily, Hourly, or Raw Data.

Network

The **Network** tab presents a top-level wireless network summary report along with additional reports on wireless mobility zones, virtual networks, controllers, and AP groups. These context sensitive reports include data-point rollovers and drill-down links to additional detailed reports, as well as the ability to launch local management.

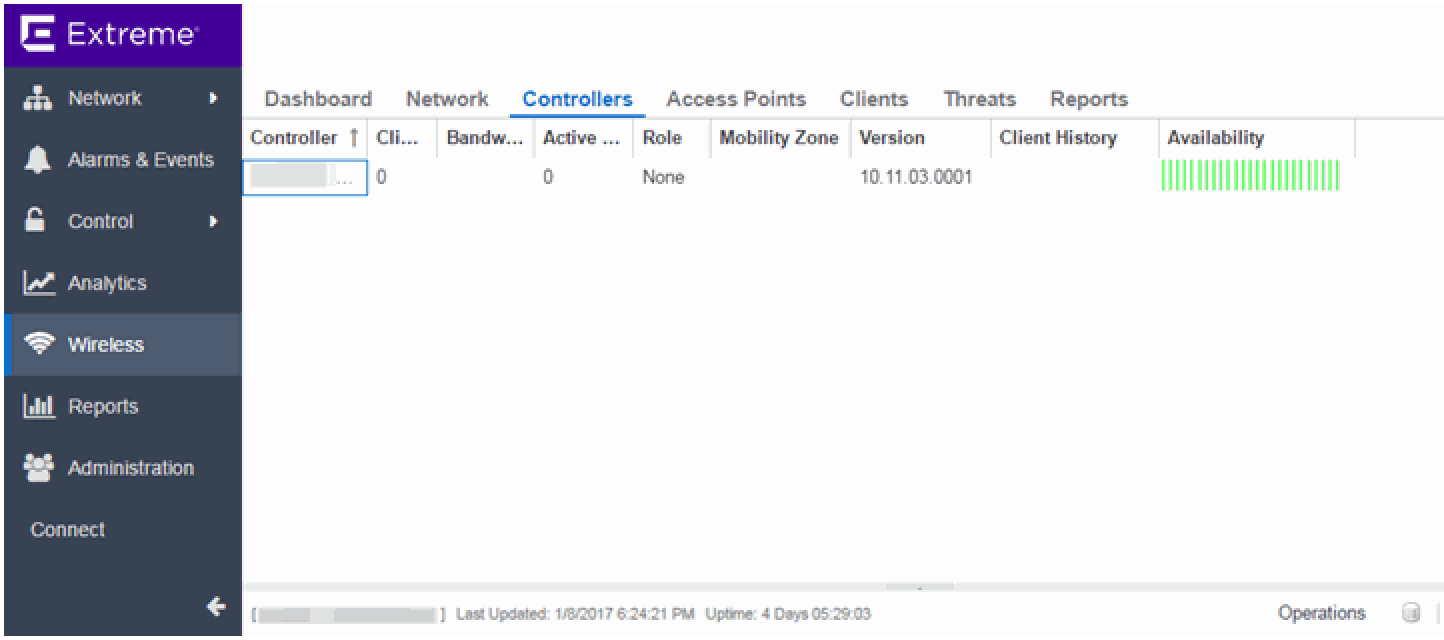
Reports are presented in a familiar wireless component tree structure similar to how components are displayed in Wireless Manager. Clicking on any node in the tree provides contextual information for that node.

Select **Discover All Controllers** in the **Tools** menu at the bottom of the tree panel to perform a discover operation that looks for any configuration changes on your wireless controllers with device statistics collection enabled. In addition, you can select **Discover Controller** to rediscover a single controller. Select the controller in the tree, click the down arrow next to the **Discover** button and select **Discover Controller**.

Click **Manage Controllers** in the menu at the bottom of the tree panel to open the ExtremeWireless Assistant where you can remotely manage your wireless controllers.

Controllers

This report displays summary information for each controller. Click on the Controller IP address link to open a report that shows APs by channel, clients by protocol, clients by WLAN, clients, and bandwidth usage information for just that controller.



Controller ↑	Cli...	Bandw...	Active ...	Role	Mobility Zone	Version	Client History	Availability
[redacted] ...	0		0	None		10.11.03.0001		

[[redacted]] Last Updated: 1/8/2017 6:24:21 PM Uptime: 4 Days 05:29:03

Access Points

This report displays summary information for all the Access Points on your wireless network. Hover over the far left column and click on the gray arrow ▼ to open the AP Details window that provides controller, bandwidth, and client information. Click on a single AP name link to open an in-depth AP Summary view for the selected AP.

Click on an AP Status icon to open a table listing the current alarms for the AP. Right-click on a single AP to access a menu of AP reports. Right-click on an AP and select **Search Maps** to open a map with the AP in the center.

Select one or more APs and use the **Menu** icon (≡) in the upper left corner (or right-click on a row) to access various reports and perform various AP actions including:

- Refreshing/rediscovering the selected APs
- Editing AP location
- Setting AP orientation
- Adding selected APs to a specified Extreme Management Center map or to maps based on AP location
- Removing selected APs from associated maps
- Searching maps for the selected APs

Clients

The Clients report provides information on wireless network clients and client events. The **Clients** sub-tab displays a list of the currently active clients on the wireless network. The **Client Events** tab shows a historical list of the add, delete, and update events for clients on the wireless network. Events are triggered by:

- Client session start and end
- Inter-AP roaming
- IP address change (including going from no IP address to having one)
- Authentication state change

Events must be collected to display event data in the **Clients** tab. To enable event collection, click the **Enable Event Collection** button at the bottom of the tab.

Select a client or client event in the report tables and use the **Menu** icon (≡) in the upper left corner to access additional reports:

- **Client History** — Opens a report displaying bandwidth, RSS, and packet statistics for the selected client. (You can also access the Client History report by clicking on a client's MAC address in the table.) From the Client History window, you can click a button to launch PortView for that client.
- **Client PortView** — Launches a PortView for the client.
- **Search Maps** — If the client is connected to a switch added to a Extreme Management Center map, the Maps sub-tab opens with the client centered on the map.
- **AP Summary** — Opens a report displaying summary statistics for the client's AP. From the AP Summary window, you can click a button to launch a Wireless AP Radio Summary report and also launch PortView for the AP device. (You can also access the AP Summary report by clicking on the AP Name link in the Client Events table.)

Use the **Search** field to search the reports by specifying an active user name or host name, MAC address, active IP address, or AP name.

Client Events Report Options

You can set data collection options for the Client Events report in the Wireless History Settings window accessed from Console OneView Collector options (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Client History and Threat options). These options include setting the maximum number of client changes to store in the history and the maximum number of client events the report can request at one time.

You can also filter client events to include or exclude certain SSIDs using the Console OneView Collector options (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Include/Exclude Filter List). This allows you to filter the history so only events for clients you are particularly interested in are displayed.

Client Location Information

Mouse over the Location column in the report tables to view a tooltip that displays whether the client's location is based on triangulated (Triangulation) or Cell of Origin data. The tooltip also displays whether the client's location is currently being tracked by the controller and if it is on the controller's on-demand list.

To track clients, enable the "Locate Active Sessions" setting in the wireless controller's Location Engine Settings. When this setting is enabled, the controller's location engine automatically tracks the location of all associated clients up to the platform's limit (e.g. 2500 stations for C5210). Even if a client has a session on a controller, if the limit has been reached, the location engine may not be tracking that particular client. Use this tooltip to determine if the client is currently being tracked.

Clients added to the controller's on-demand list are always tracked, regardless of whether tracking is enabled and any platform limits. Place clients that require guaranteed location history on the controller's on-demand list, configured in the controller's Location Engine Settings. Clients on this list also receive better location detection than other tracked clients, minimizing the number of Cell of Origin location results.

For more information on configuring controller Location Engine Settings and on-demand lists, refer to the *Extreme Networks Convergence Software User Guide*. Refer to the section on "Configuring the Location Engine" in the Working with ExtremeWireless Radar chapter.

Event Analyzer

The Event Analyzer tab provides information about wireless end-points connecting to your network.

Threats

These reports show devices detected by the Radar WIDS-WIPS system as sources of threats or interference on the wireless network.

A threat source is a device detected to be performing one or more types of attacks on the wireless network.

An interference source is a device generating a radio signal interfering with the operation of the wireless network. An example of an interference source is a microwave oven, which can interfere with 2.4GHz transmissions.

There are four sub-tabs displaying active and historic data:

- Threats — Lists only currently active threats.
- Threat Events — Lists a historic record of threat events including active threats.
- Interference — Lists only currently active sources of interference.

- Interference Events — Lists a historic record of interference events including active sources of interference.

NOTE: You can set the maximum number of threat events to store in history in Console (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Client History and Threat options).

Following are definitions of the table columns and fields displayed in the sub-tabs.

Status

The status of the threat or source of interference.

- Active — An active threat or source of interference on the network.
- Inactive — A threat or source of interference no longer active on the network.
- Aged — A threat or source of interference not reported by Radar as having gone away and has not been seen for more than an hour.

Type

The type of threat or interference detected. Threats with no type display their category.

Categories

Individual threat types are grouped into the following categories:

- Ad Hoc Device — A device in ad hoc mode can participate in direct device-to-device wireless networks. Devices in ad hoc mode are a security threat because they are prone to leaking information stored on file system shares and bridging to the authorized network.
- Cracking — This refers to attempts to crack a password or network passphrase (such as a WPA-PSK). The Chop-Chop attack on WPA-PSK and WEP is an example of an active password cracking attack.
- Denial of Service (DoS) attacks
- External Honeypot — An AP attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport.
- Internal Honeypot — An AP attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.

- Performance — Performance issues pertain to overload conditions that cause a service impact. Performance issues aren't necessarily security issues, but many types of attacks do generate performance issues.
- Prohibited Device — A MAC address or BSSID is detected that matches an address entered manually into the Radar database.
- Spoofed AP — An AP not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
- Client Spoof — A device using the MAC address of another typically authorized station.
- Surveillance — A device or application probing for information about the presence and services offered by a network.
- Chaff — An attack that overloads a WIDS-WIPS causing it to miss more serious attacks or to go out of service. FakeAP is an example of a chaff attack.
- Unauth Bridge — A device that forwards packets between networks without authorization to do so.
- Injection — The attacker inserts packets into the communication between two devices so the devices believe the packet is coming from an authorized device.

MAC Address

The MAC address to which this threat event applies. In the case of Spoofed AP, Internal Honeypot, or External Honeypot, it is the advertised BSSID of the threat AP.

Start Time

The date and time the threat or source of interference is identified.

Stop Time

The date and time the threat or source of interference stopped.

Countermeasures Applied

Countermeasures the AP is taking against the threat. These include:

- Prevent authorized stations from roaming to external honeypot APs.
- Prevent any station from using an internal honeypot AP.
- Prevent authorized stations from roaming to friendly APs.
- Prevent any station from using a spoofed AP.
- Drop frames in a controlled fashion during a flood attack.
- Remove network access from clients in ad hoc mode.

- Remove network access from clients originating DoS attacks.
- None

AP Name

Name of the AP reporting the threat or source of interference. Click on the link to open the AP Details window that provides controller, bandwidth, and client information.

From the AP History sub-tab, click the **Gear** menu ≡ in the upper right corner of the window to access a menu of additional AP reports.

RSS

Receive signal strength (in dBm) of the threat or source of interference.

Additional Details

Additional information including:

- frequency=<channel> or NA
- SSID=<SSID name>
- encryption=<WEP/WPA1/WPA2/WPA12>

Search

Use the **Search** field at the top right of the window to search by threat type, threat category, MAC address, or AP name.

Refresh Interval

Use the **Refresh** drop-down menu at the top right of the window to specify an interval (in seconds) at which the threat or interference data is automatically refreshed. To stop auto refresh, select the **Refresh Off** option.

Search Maps

To locate an AP on a map, right-click on a threat and select **Search Maps**. If the AP is added to a map, the map opens with the AP centered on the map.

Reports

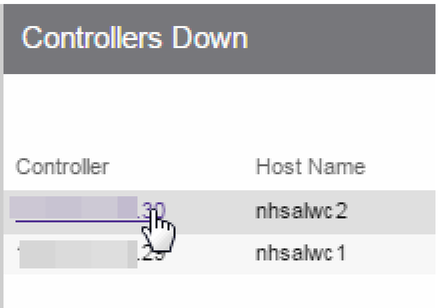
The **Reports** tab allows you to view information about the APs, controllers, and wireless traffic on your network. Available reports are accessible via the **Reports** drop-down menu at the top of the tab.

Click the **Export to CSV** button (X) to export the information contained in the report to your default CSV application, where it can then be manipulated or saved.

Report Features

Extreme Management Center reports include the following features (depending on the report selected):

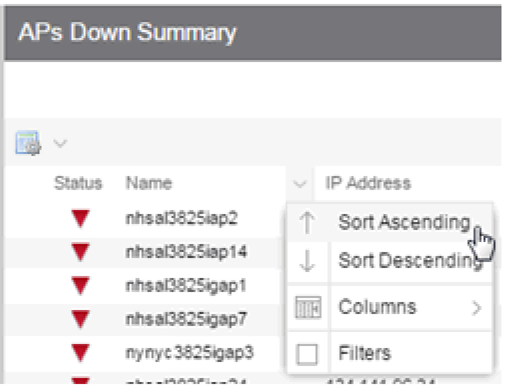
- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



Controllers Down

Controller	Host Name
[redacted]	nhsalwc2
[redacted]	nhsalwc1

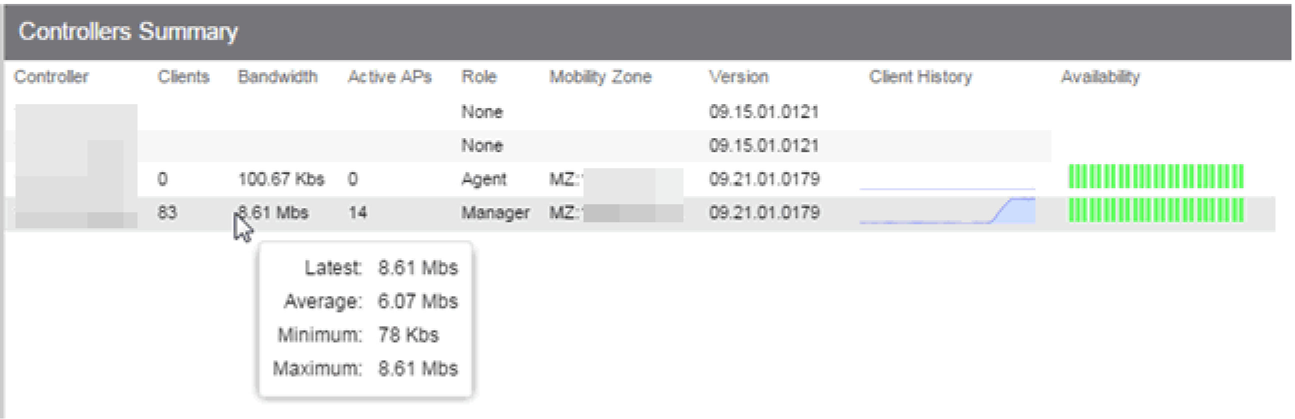
- **Interactive Tables** — Manipulate table data in several ways to customize the view for your own needs:
  - Click on the column headings to **perform an ascending or descending sort** on the column data.
  - **Hide or display different columns** by clicking on a column heading drop-down arrow and selecting the column options from the menu.
  - **Filter, sort, and search** the data in each column in the table.



APs Down Summary

Status	Name	IP Address
▼	nhsal3825iap2	
▼	nhsal3825iap14	
▼	nhsal3825igap1	
▼	nhsal3825igap7	
▼	nynyc3825igap3	

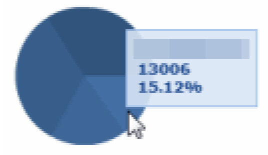
- **Interactive Charts** — Use data-point rollovers for quick information on chart data. For example, in the Controller Summary report, rolling over the value reported for Bandwidth provides additional bandwidth statistics over time.



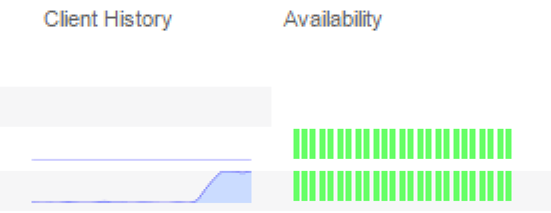
Controllers Summary

Controller	Clients	Bandwidth	Active APs	Role	Mobility Zone	Version	Client History	Availability
[redacted]				None		09.15.01.0121		
				None		09.15.01.0121		
	0	100.67 Kbs	0	Agent	MZ:[redacted]	09.21.01.0179		
	83	8.61 Mbs	14	Manager	MZ:[redacted]	09.21.01.0179		

Latest: 8.61 Mbs
Average: 6.07 Mbs
Minimum: 78 Kbs
Maximum: 8.61 Mbs



- Sparkline Charts — View network trends in dense, succinct charts that present report data in an easy to read, condensed format. This provides you with a quick way to catch possible problem areas that you can investigate further. Rollover charts for additional information.



Related Information

For information on related Extreme Management Center topics:

- Administration
- Network
- Alarms and Events
- Reports
- Search

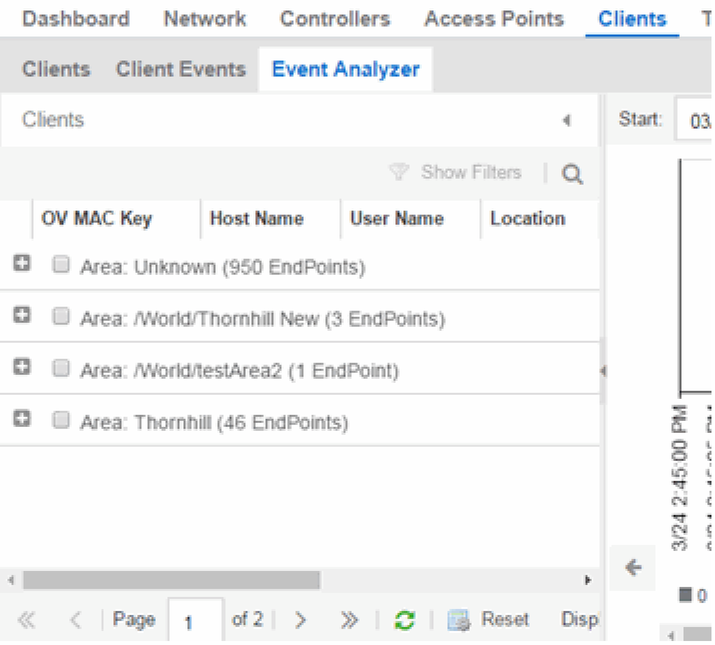
Event Analyzer

The **Event Analyzer** tab provides information about events caused by wireless end-points connecting to your network.

You can access the tab in a number of ways and the information presented changes depending on the method you use:

- Navigating via **Wireless** > **Clients** > **Event Analyzer** shows all end-points.
- Clicking a Location on the **Wireless** > **Clients** tab opens the Event Analyzer for the end-points that occurred for all APs in that Location.
- Clicking a MAC address on the **Wireless** > **Clients** tab opens the Event Analyzer for only that end-point.

When accessing the tab using the top two methods, a Clients section is available in the left-panel. This section provides you with the ability to display end-point events for specific AP locations.

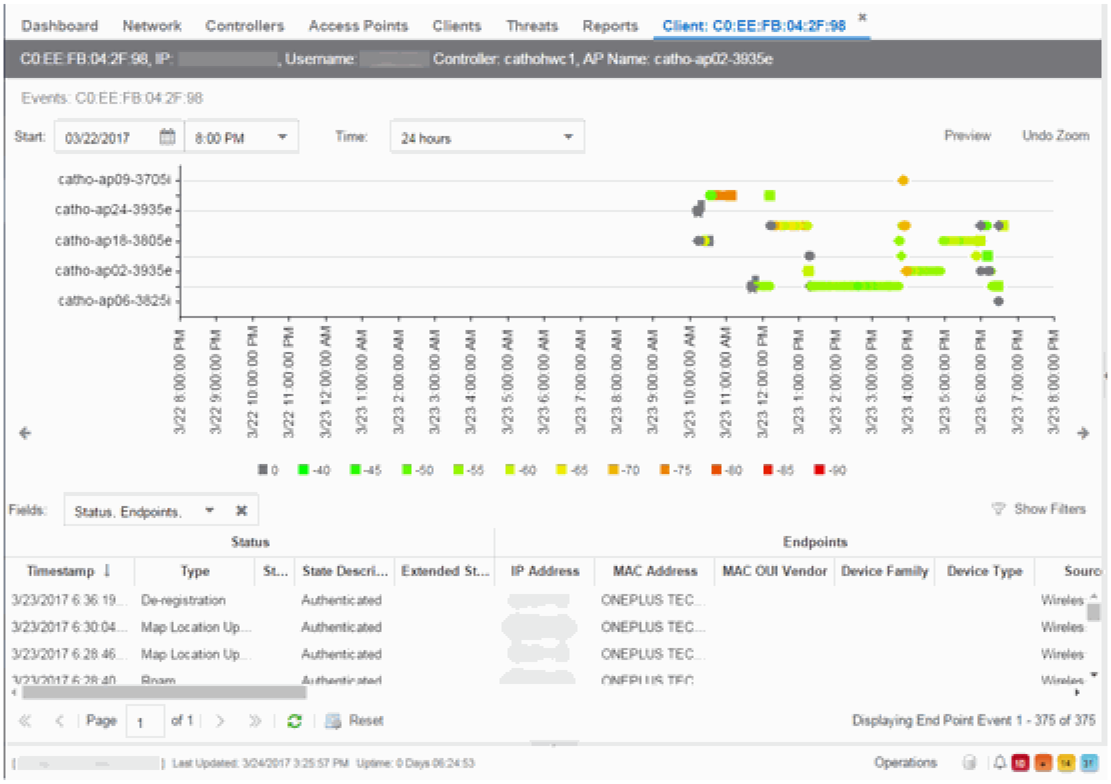


OV MAC Key	Host Name	User Name	Location
☐ Area: Unknown (950 EndPoints)			
☐ Area: /World/Thornhill New (3 EndPoints)			
☐ Area: /World/testArea2 (1 EndPoint)			
☐ Area: Thornhill (46 EndPoints)			

Once you select the appropriate end-points or areas, this section can be collapsed by clicking the left arrow.

The top of the tab contains a graph displaying the RSS (Received Signal Strength) for the end-point events.

The bottom contains a table showing information about each event.



C0:EE:FB:04:2F:98, IP: [redacted], Username: [redacted] Controller: cathohwc1, AP Name: catho-ap02-3935e

Events: C0:EE:FB:04:2F:98

Start: 03/22/2017 8:00 PM Time: 24 hours

Fields: Status, Endpoints,

Status					Endpoints					
Timestamp	Type	St...	State Descri...	Extended St...	IP Address	MAC Address	MAC OUI Vendor	Device Family	Device Type	Sourc
3/23/2017 6:36:19...	De-registration		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:30:04...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:28:46...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:28:40...	Roam		Authenticated		[redacted]	ONEPLUS TEC				Wireles

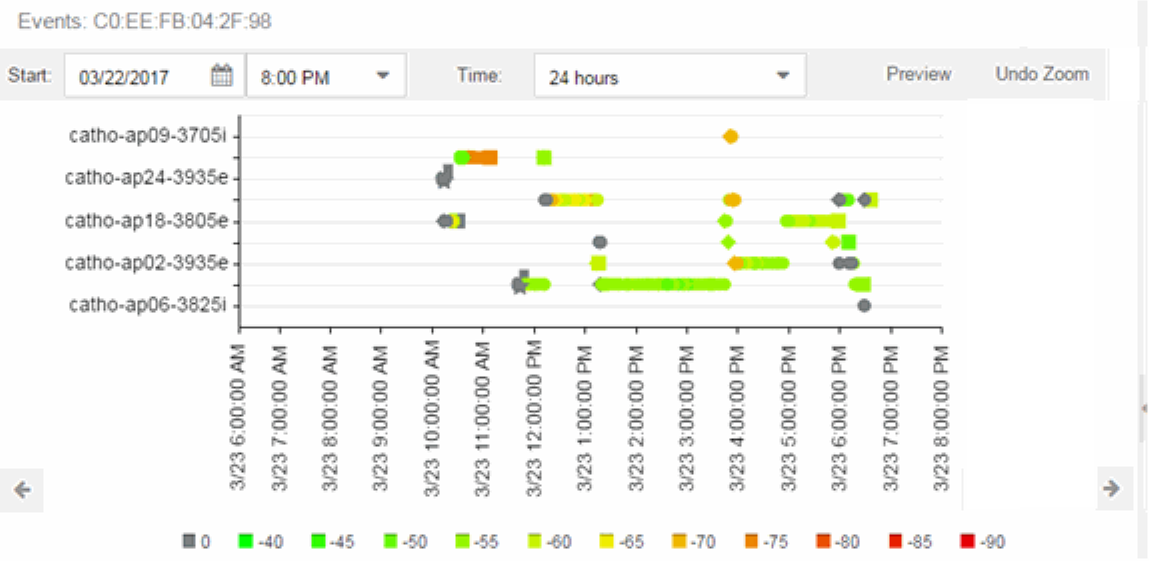
Page 1 of 1

Displaying End Point Event 1 - 375 of 375

Last Updated: 3/24/2017 3:25:57 PM Uptime: 0 Days 06:24:53

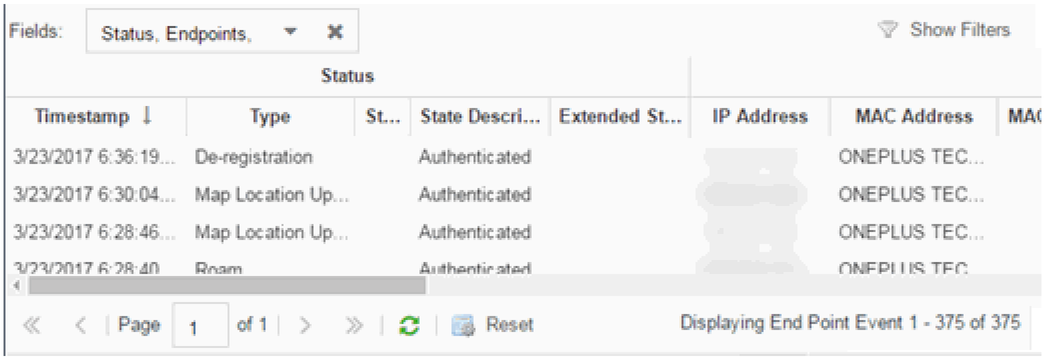
RSS Graph

The RSS graph at the top of the tab shows the signal strength (in dBm) between the end-point and each of the APs to which it connected. The shape of the end-point event indicators in the graph indicate the type of event.



Events Table

The Events table at the bottom of the tab contains details about the end-point events for your network, or for the wireless location or MAC address you selected.



Status							
Timestamp ↓	Type	St...	State Descri...	Extended St...	IP Address	MAC Address	MA(
3/23/2017 6:36:19...	De-registration		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:30:04...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:28:46...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:28:40	Roam		Authenticated		[redacted]	ONEPLUS TEC	

Displaying End Point Event 1 - 375 of 375

Use the **Fields** drop-down menu to select groups of columns to display in the table:

- Select **Status** to display the following columns in the table:
  - Timestamp
  - Type
  - State

    - State Description
    - Extended State
- Select **Endpoints** to display the following columns in the table:
    - IP Address
    - OV MAC Key
    - MAC Address
    - MAC OUI Vendor
    - Host Name
    - Device Family
    - Device Type
    - Source
- Select **User Access** to display the following columns in the table:
    - User Name
    - Policy
    - Authorization
    - Profile
    - Reason
    - Auth Type
    - Registration Type
    - RADIUS Server IP
- Select **Location** to display the following columns in the table:
    - Switch Port
    - Switch Port Index
    - Switch Location
    - AP Name
    - AP Serial #
    - BSSID
    - SSID
    - Protocol
    - Location Type

    - Location
    - Location Details
    - Area Type
    - Area
    - Extreme Access Control Engine/Source IP
- Select **Metrics** to display the following columns in the table:
    - RSS
    - SNR
- Select **Threat/Risk** to display the following columns in the table:
    - Categories
    - Start Time
- Select **Network Service** to display the following columns in the table:
    - Switch IP
    - Controller IP

Related Information

For information on related Extreme Management Center topics:

- Wireless

Governance Overview

The Extreme Management Center **Governance** tab provides oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.

IMPORTANT: The **Governance** tab is available and supported by Extreme on an Extreme Management Center engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Governance functionality, but python version 2.7 or higher must be installed. Additionally Governance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Run a governance audit against devices on the **Governance** tab or against device archives on the **Network** > Archives tab.

NOTE: **Governance** tab functionality requires you to acquire an additional license.

Extreme Management Center provides a set of audit tests that allow you to test the configuration of your devices. Groups of audit tests comprise a regime, which tests for a specific regulation or standard. Extreme Management Center uses the results to determine a score that indicates compliance with a regulation or standard.

The regimes included in the **Governance** tab are automatically included in your Extreme Management Center version 8.1 installation on an Extreme Management Center engine, but you must import them on a non-Extreme Management Center engine by accessing the engine console, navigating to the `<`*`install directory`*`>/GovernanceEngine` directory and entering `./governance-engine.py --db-import-all-tests --governance-type PCI` to import the PCI regime and `./governance-engine.py --db-import-all-tests --governance-type HIPAA` to import the HIPAA regime.

Configure a regime by disabling or editing specific audit tests within the regime. Once the regime meets your needs, use it to run a governance audit against a device or set of devices. You cannot run individual audit tests against a device.

The **Governance** tab contains the following sub-tabs:

- Dashboard
- Audit Tests

Dashboard

The Dashboard tab displays an overview of the audit test results for each regime. Additionally, the tab provides information about how the regime test results changed over time, the performance of each of the devices included in the audit test, and a list of the tests performed as part of the regime.

Audit Tests

The Audit Tests tab contains a variety of audit tests organized into the regime or standard of which it is a part. You can also create your own audit tests for the devices on your network via the **Audit Tests** tab.

Audit tests can be run ad-hoc or on a scheduled basis. Use the results to ensure your devices are configured to industry standards and are safe from vulnerabilities.

Related Information

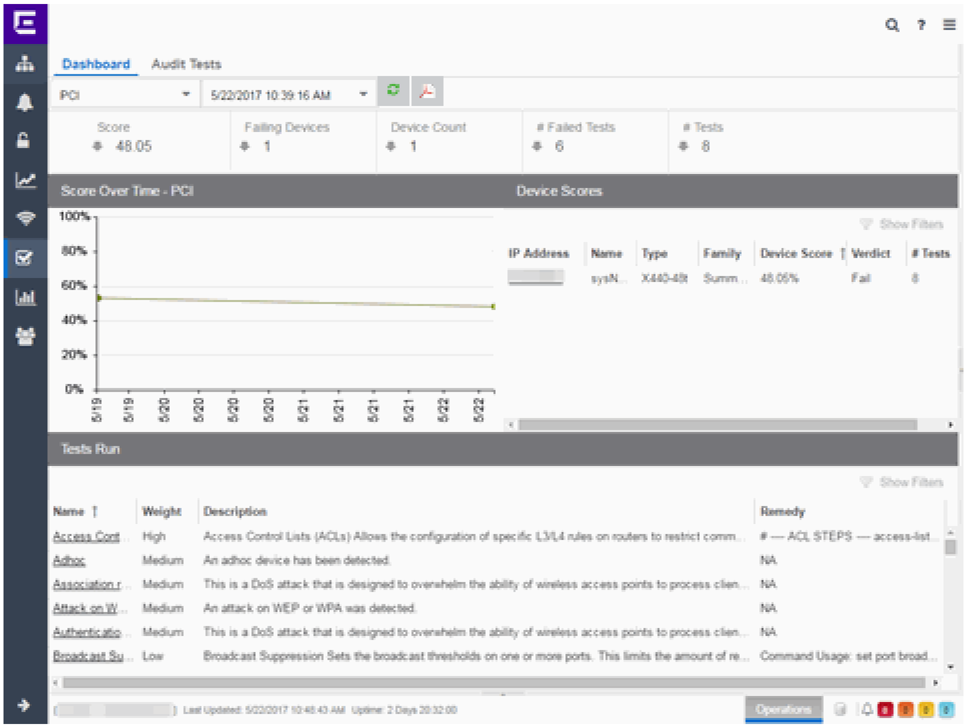
For information on related tabs:

- Governance Dashboard
- Audit Tests
- Archives

Governance Dashboard

The **Governance** > **Dashboard** tab provides an overview of your audit test results performed over time on the devices in your network.

Use the drop-down menus at the top of the tab to select the regime and the date and time of the governance audit to view the results in the tab. Click the **Export to PDF** icon () to produce a PDF report that provides a summary of the regime audit test and a breakdown of the results for each device included in the test.



PCI | 5/22/2017 10:39:16 AM

Score	Failing Devices	Device Count	# Failed Tests	# Tests
48.05	1	1	6	8

IP Address	Name	Type	Family	Device Score	Verdict	# Tests
[redacted]	sysN...	X440-48t	Summ...	48.05%	Fail	8

Name	Weight	Description	Remedy
Access Cont...	High	Access Control Lists (ACLs) Allows the configuration of specific L3/L4 rules on routers to restrict comm...	# — ACL STEPS — access-list...
Adhoc	Medium	An adhoc device has been detected.	NA
Association r...	Medium	This is a DoS attack that is designed to overwhelm the ability of wireless access points to process clien...	NA
Attack on W...	Medium	An attack on WEP or WPA was detected.	NA
Authenticatio...	Medium	This is a DoS attack that is designed to overwhelm the ability of wireless access points to process clien...	NA
Broadcast Su...	Low	Broadcast Suppression Sets the broadcast thresholds on one or more ports. This limits the amount of re...	Command Usage: set port broad...

[redacted] Last Updated: 5/22/2017 10:48:43 AM Uptime: 2 Days 20:32:00

Test Results

The top of the **Dashboard** tab displays the audit test results for the governance audit you select using the regime and date in the drop-down menu.

Score

The number in this field is an average of the scores on each device included in the audit. Each device earns a score by comparing the percentage of audit tests that ran successfully on the device to the total number of audit tests. Clicking the score opens the **Run Results** tab, which provides a list of all of the audit tests run on all of the devices included in the audit, including the results.

Failing Devices

The number of devices that failed the governance audit. Clicking the number of failing devices opens the **Device Scores** tab, which provides a list of the devices that failed the audit test.

Device Count

The total number of devices included in the governance audit. Clicking the device count opens the **Device Scores** tab, which provides a list of all of the devices included in the audit test.

# Failed Tests

The number of tests that failed when run against devices included in the governance audit. Clicking the failed test number opens the **Run Results** tab, which provides a list of the audit tests that failed when run on a device included in the audit.

# Tests

The total number of tests run against devices included in the governance audit. Clicking the number of tests opens the **Run Results** tab, which provides a list of all audit tests run on devices included in the audit.

Score Over Time

The Score Over Time graph shows the results of all of the audit tests performed on your devices for the regime selected in the drop-down menu at the top of the window. This allows you to determine any trends and map your progress towards compliance with a particular regime.

Device Scores

The Device Scores section of the tab displays a table of the devices included in the audit test, details about those devices, and the results of the governance audit on each device.

IP Address

The IP address of the device tested.

Clicking an address in the IP Address column opens that device in the **Device Details** tab, which provides governance audit result information for that device.

Name

The name of the device, configured in the **System Name** field in the Configure Device window.

Type

The specific type (model) of the device.

Family

The group of devices to which the device belongs, known as the device family in Extreme Management Center.

Device Score

The percentage of audit tests within the regime with which the device passes compliance. For example, if a device complies with 75 out of 100 audit tests in a regime, the **Device Score** is **75%**.

Verdict

The result of the governance audit (either **Pass** or **Fail**), based on the Device Score. A device with a score of less than 50% is labeled as **Fail** in the Verdict column, while a score of 50% or above is considered a **Pass**.

# Tests

The number of tests included in the governance audit run against the device.

Tests Run

The Tests Run table displays a list of all of the tests included in the regime selected at the top of the window. The section also contains details about each of the audit tests and the action you can take to correct the device in the event that your device fails a test.

Clicking the test name in the **Name** column opens the **Test Details** tab, which provides information about the results of the test on all devices both over time and during a particular governance audit.

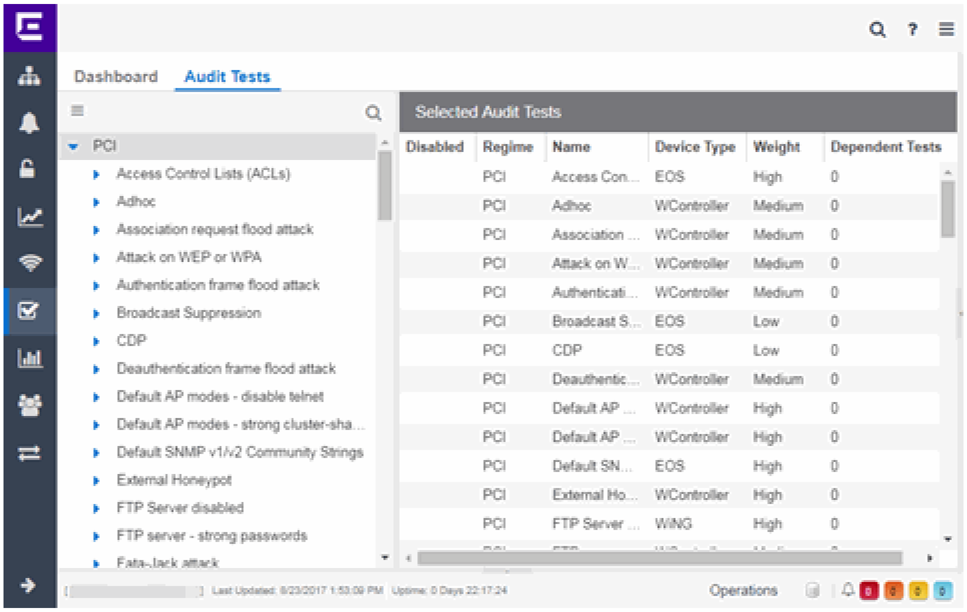
Related Information

For information on related topics:

- Governance
- Audit Tests
- Configure Device

Audit Tests

The **Audit Tests** tab displays a set of audit tests that check for vulnerabilities in your devices. The tab also allows you to create your own audit tests you can add to regimes.



- PCI
  - Access Control Lists (ACLs)
  - Adhoc
  - Association request flood attack
  - Attack on WEP or WPA
  - Authentication frame flood attack
  - Broadcast Suppression
  - CDP
  - Deauthentication frame flood attack
  - Default AP modes - disable telnet
  - Default AP modes - strong cluster-sha...
  - Default SNMP v1/v2 Community Strings
  - External Honeypot
  - FTP Server disabled
  - FTP server - strong passwords
  - Fata-Jack attack

Disabled	Regime	Name	Device Type	Weight	Dependent Tests
	PCI	Access Con...	EOS	High	0
	PCI	Adhoc	WController	Medium	0
	PCI	Association ...	WController	Medium	0
	PCI	Attack on W...	WController	Medium	0
	PCI	Authenticati...	WController	Medium	0
	PCI	Broadcast S...	EOS	Low	0
	PCI	CDP	EOS	Low	0
	PCI	Deauthentic...	WController	Medium	0
	PCI	Default AP ...	WController	High	0
	PCI	Default AP ...	WController	High	0
	PCI	Default SN...	EOS	High	0
	PCI	External Ho...	WController	High	0
	PCI	FTP Server ...	WiNG	High	0

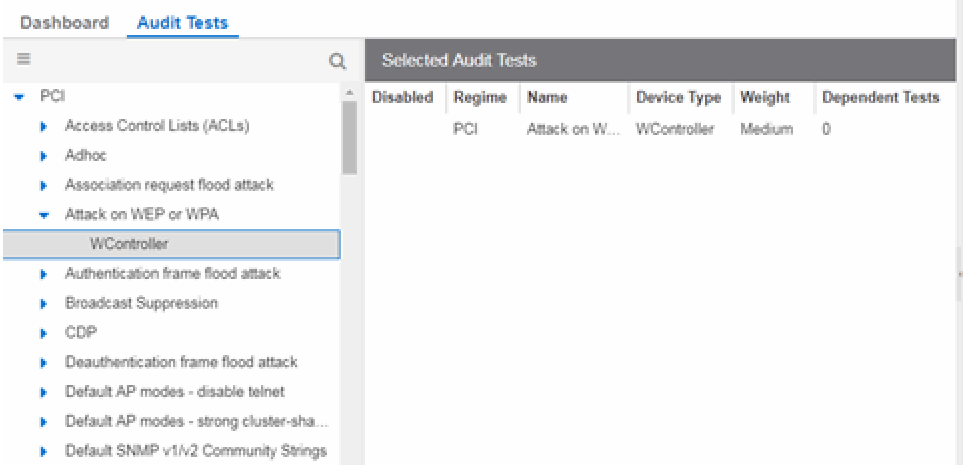
Last Updated: 8/23/2017 1:53:09 PM Uptime: 0 Days 22:17:24

The Audit Test list contains a list of all of the audit tests available in Extreme Management Center, contained within the regulatory and standards regime of which it is a part. Each individual audit test contains the device types on which the test can be run.

Select a regime, audit test, or device type in the Audit Test list to view the details of any audit tests contained in that folder in the Selected Audit Tests table to the right of the tree. Click the **Magnifying Glass** icon (🔍) and begin typing to search within the regimes for a specific audit test.

Disable an audit test by right-clicking it in the left-panel and selecting **Disable Audit Test**. Delete an audit test by right-clicking it in the left-panel and selecting **Delete Audit Test**.

NOTE: Only user-created audit tests or audit tests in user-created regimes can be deleted. Additionally, only user-created regimes can be deleted.


Dashboard
Audit Tests
PCI
Access Control Lists (ACLs)
Adhoc
Association request flood attack
Attack on WEP or WPA
WController
Authentication frame flood attack
Broadcast Suppression
CDP
Deauthentication frame flood attack
Default AP modes - disable telnet
Default AP modes - strong cluster-sha...
Default SNMP v1/v2 Community Strings
Selected Audit Tests

Disabled	Regime	Name	Device Type	Weight	Dependent Tests
	PCI	Attack on W...	WController	Medium	0

Disabled

A checkmark in this column indicates the test is disabled for the regime. When a test is disabled, it is not run when performing a governance audit against a device or a group of devices. To disable or enable an audit test, select the test in the left-panel, right-click the audit test, and select Disable Audit Test or Enable Audit Test, respectively.

Regime

This indicates standard or regulation to which you are maintaining compliance. Each regime contains a set of audit tests, specific to a device type. Expand the regime folder to view the tests included as part of the regime.

Selecting a regime opens a list of all of the audit tests in that regime in the selected Audit Tests table to the right of the list. Use the Selected Audit Tests table to select or deselect any of the tests in the regime and then run an audit test using all of the selected tests in the regime on the devices you select to which the tests apply.

Name

This shows the name of the audit test, a test of the configuration of a device to ensure compliance with the best practices of that industry and is nested within the regime to which the test applies. Expand the audit test folder to see the device types to which that test applies.

Device Type

The device type displays the type of devices on which you can run the expanded audit test and is the lowest level in the Audit Test list, nested within an audit test.

Selecting device type displays that audit test in the Details table to the right of the Audit Test list. Use the Details table to select or deselect the test and then run an audit test on the devices you select to which the test applies.

Additionally, double-clicking the device type from the left-panel opens the Edit Audit Test window from which you can edit the audit test.

Weight

The value in the **Weight** column of the Selected Audit Tests table indicates the priority of the audit test:

- High
- Medium
- Low

Dependent Tests

This shows the number of audit tests that must run successfully before the selected test runs.

For example, when running an audit test to ensure a device is running the latest version of an anti-virus software, you might first check whether the device has anti-virus software installed. The audit test verifying the version does not run if the audit test checking whether an anti-virus software is installed fails.

Use the **Menu** icon (≡) in the left-panel to add a new regime or audit test, edit existing regimes or audit tests, or run the regime against a device or group of devices. These options are also available via the right-click menu in the left-panel.

Select a regime from the left-panel, click the **Menu** icon and select **Run Regime** to open the **Run Regime** window, where you select the device against which to run the audit.

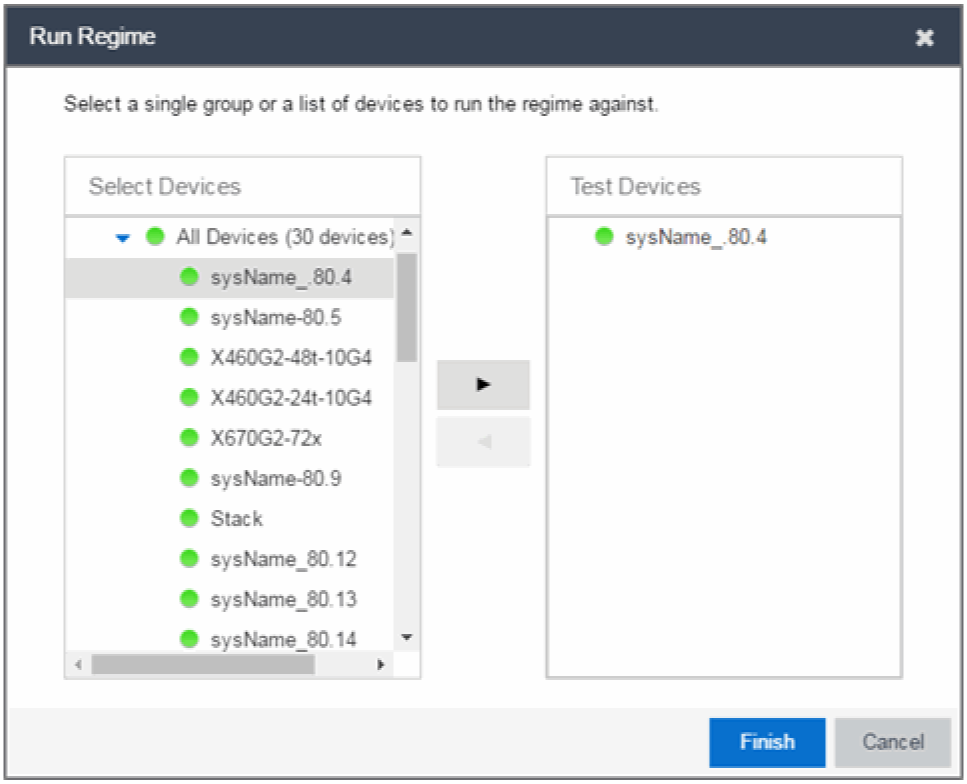
Related Information

For information on related tabs:

- Governance
- Scheduler

Run Regime

This window allows you to select the device or devices against which to run the selected audit test. The **Run Regime** window contains all of the devices added to Extreme Management Center.



Run Regime

Select a single group or a list of devices to run the regime against.

Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Click the right arrow button **>** to move the devices to the Test Devices list.

Test Devices

Lists the device(s) or device group the on which the audit test is performed. To remove a member from the list, select the device or device group and click the left arrow button **<**.

Right Arrow Button

Click **>** to add the device(s) or device group to the Test Devices list.

Left Arrow Button

Click **<** to remove the device(s) or device group from the Test Devices list.

Finish Button

Click the **Finish Test** button to run the selected audit test(s) on the devices selected in the Test Devices list. The progress of the governance audit is displayed in the Operations table.

Related Information

For information on related tabs:

- Governance
- Scheduler

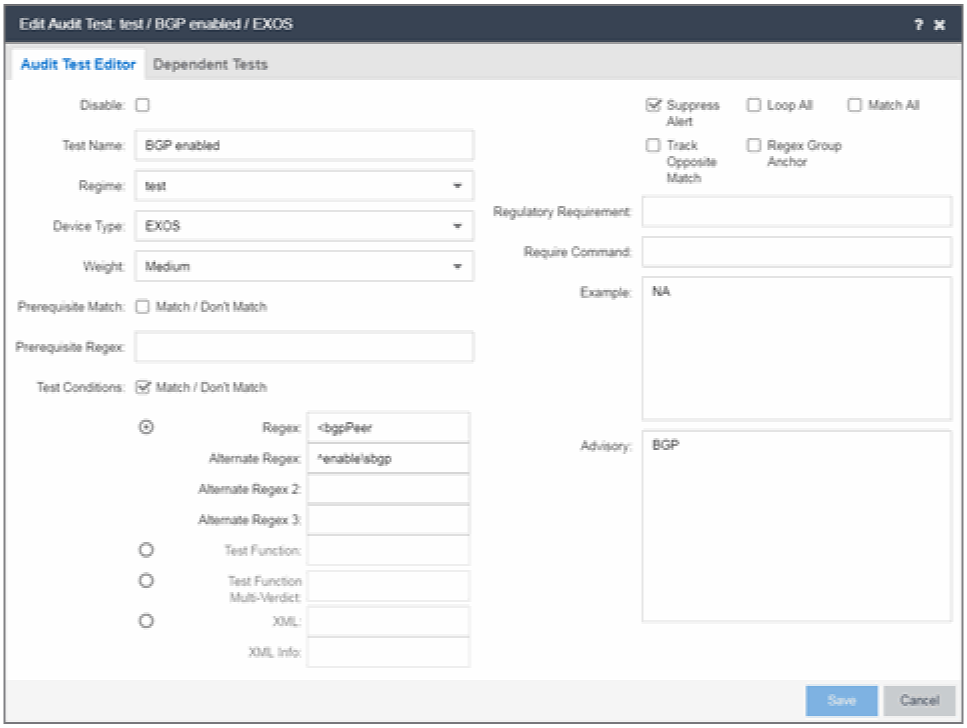
Create/Edit Audit Test

Use the **Audit Test Editor** tab of the **Create/Edit Audit Tests** window to create a new audit test or edit information for an existing audit test. The **Audit Test Editor** tab in the Create/Edit Audit Test window allows you to indicate the name of the audit test, the regime to which it belongs, the device type to which the test applies, and the weight of the test.

Access the Create Audit Test window on the **Governance** > Audit Tests tab by selecting a regime in the left-panel, clicking the **Menu** icon (≡), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, clicking the **Menu** icon (≡), and selecting **Edit** > **Audit Test**.

NOTE: Only audit tests in user-created regimes can be edited.



Edit Audit Test: test / BGP enabled / EXOS

Audit Test Editor | Dependent Tests

Disable: □

Test Name: BGP enabled

Regime: test

Device Type: EXOS

Weight: Medium

Prerequisite Match: □ Match / Don't Match

Prerequisite Regex:

Test Conditions: ☑ Match / Don't Match

● Regex: <bgpPeer

Alternate Regex: ^enable\sbgp

Alternate Regex 2:

Alternate Regex 3:

○ Test Function:

○ Test Function Multi-Verdict:

○ XML:

XML Info:

☑ Suppress Alert □ Loop All □ Match All

□ Track Opposite Match □ Regex Group Anchor

Regulatory Requirement:

Require Command:

Example: NA

Advisory: BGP

Disable

Select the checkbox prevent the audit test from running as part of the regime when a governance audit is performed on your devices.

Test Name

The name of the audit test. As regimes contain a large number of audit tests, some of which testing similar configurations, ensure the Test Name is very specific.

Regime

The set of standards or regulations to which the test applies. Extreme Management Center comes with three regimes, PCI, HIPAA, and GDPR. You can create a new regime or edit an existing regime on the Audit Tests tab by clicking the Menu icon and selecting Add or Edit > Regime.

Device Type

The type of device being tested. In version 8.1, Extreme Management Center supports multiple Device Types, including E200, EXOS, EOS, BOSS, VOSS, and WController.

Weight

The priority of the audit test. Valid selections are Low, Medium, or High.

Prerequisite Match

Select this checkbox to indicate the regular expression or function audit test must match the configuration file for the audit test to be valid.

Prerequisite Regex

The regular expression that must match the device configuration file for Extreme Management Center to consider the audit test valid.

For example, if an audit test is checking if strong ciphers are selected for SSH configuration, use this field to verify that SSH is enabled.

Match

Select this checkbox to indicate the regular expression or function audit test are intended to match the configuration file to be compliant and pass the test. If the checkbox is not selected, any result that does not match the test case is considered compliant and passes the test.

Regex

The regular expression against which Extreme Management Center is comparing a device's configuration file.

Alternate Regex

A second regular expression against which Extreme Management Center is comparing a device's configuration file, in case the Regex test fails.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS configuration files use both XML and plain text).

Alternate Regex 2

A third regular expression against which Extreme Management Center is comparing a device's configuration file, in case the other **Regex** tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS configuration files use both XML and plain text).

Alternate Regex 3

A fourth regular expression against which Extreme Management Center is comparing a device's configuration file, in case the other **Regex** tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS configuration files use both XML and plain text).

Test Function

A python function you can configure if the audit test requires more complex logic to test a configuration.

Test Function Multi-Verdict

A python function you can configure to return multiple verdicts. Use this to configure audit tests for wireless controllers with complex configurations.

XML

Select the button and enter the XML element in the wireless threat data for which the audit test is checking.

XML Info

Enter the set of `Info` elements from the wireless threat XML data for which the audit test is checking.

Supress Alert

Select this checkbox to indicate the result of the audit test is not factored into the score assigned to the devices included in a governance audit.

Loop All

Select this checkbox to indicate the audit test is performed repeatedly against the entire device configuration and the match criteria is applied to the end result of the governance audit. For example, if SSH must be enabled in multiple places on a device, selecting this checkbox requires SSH to be enabled in all places to pass.

Match All

Select this checkbox to indicate all instances of the regular expression you are comparing to the device configuration must match for the audit test to pass.

Track Opposite Match

Select this checkbox if you want the results of the audit test to indicate whether the opposite of the regular expression you are comparing to the device configuration is observed during the governance audit.

Regex Group Anchor

Select this checkbox to indicate this audit test is the starting point for the regime. Use this checkbox for test chains when collecting data via regex capture groups.

Regulatory Requirement

The requirement from the standard or regulation that serves as the justification for the audit test.

Require Command

The path to a command on the Extreme Management Center server, if required for the audit test. For example, enter the path to the `cracklib-check` command for an audit test verifying the strength of cleartext credentials.

Example

A descriptive example of the configuration for which the audit test is checking.

Advisory

The reason the audit test is important to the regulation or standard and the procedure to improve the audit test results.

Related Information

For information on related topics:

- Audit Tests
- Dependent Tests

Reports

Extreme Management CenterReports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

From the **Reports** tab, you have three options:

- Reports — Select from a catalog of reports, many of which are interactive, allowing you to adjust the data and time on which to report. See below for a description of each report and a section on helpful report features and functionality. Use the **Info** button ℹ at the top-right of the Extreme Management Center page to access detailed information about many of the reports.
- Custom Report — Create your own custom report by selecting a specific target type (such as Interface, Wireless AP, or Identity and Access end-system) and a statistic based on the selected target. Display options let you display the report as a table or a chart, specify a chart type (column or line), add table titles and chart/axis titles, and assign custom colors to data series inside a chart. Click the **Info** button ℹ at the top-right of the Extreme Management Center page to access detailed information about custom report options.
- Report Designer — Create a custom dashboard report accessible from the **Reports** tab.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Requirements

To view all reports on the **Reports** tab, you must be a member of an authorization group assigned full read access capabilities to all of the Extreme Management Center tabs and reports. For more information on authorization capabilities, see the Help topic, "How to Configure User Access to Extreme Management Center Applications," located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

To collect data in your Extreme Management Center reports, you must enable statistics and flow collection for your network devices, interfaces, and wireless clients. For instructions, see How to Enable Data Collection.

Reports

The Reports catalog lets you select a report from the following report types:

- **Extreme Access Control** — Provides an overview of end-system connection information. You can also see these reports and others on the **Control** tab.
- **Extreme Access Control Health** — Provides reports on end-system assessment and state information. In the Risk Level pie chart, click on a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.
- **Extreme Access Control System** — Provides a report of the top ten end-systems by engine.
- **Application Analytics** — These reports provide visibility into the applications on your network and who's using those applications.
- **Console** — The NMS Dashboard report provides summary NMS data including top 5 switch, interface, and host statistics as well as important Wireless data. Host data is collected from network devices that support the Host Resource MIB, such as Extreme Management Center engines, Linux systems, and Windows PCs. For more information, click the **Info** button (ℹ) at the top-right of the **Reports** tab.
- **Data Center Manager** — The DCM reports provide an overview of all virtual machines on the network broken down into VM distribution per Identity and Access profile, Operating System, Switch, and Hypervisor technology. They also provide table reports with detailed information on all VMs. For each supported Hypervisor technology, sub-reports provide more in-depth data.
- **Device** — The Device reports provide information on device alarms, device archives (archive events and details), device availability, down devices, inventory summary (including archive distribution, devices backed up, database properties, scheduled events, asset tracking information, and the ability to track the changes made to a specific device), top devices by IPv6 traffic, top hosts by resource (memory, CPU, and disk usage), top switches by power (percent usage and consumption in watts), and top switches by resource (CPU and physical memory).
- **Interface** — These reports present information on your top interfaces by active flows, bandwidth, bandwidth summary, least availability, POE usage, and utilization.
- **OpenScape** — The OpenScape LIA (Location and Identity Assurance) report provides an overview of all OpenScape phones on the network categorized by phone count, phone type, phone software version, and phone distribution by access switch, as well as a list of phone information by MAC address.

- **Policy** — Provides a policy rule hit summary report showing top services and roles by rule hits.
- **Server** — These reports provide data on the Extreme Management Center server, including the Event Log, CPU and heap memory utilization, and disk access information. The information in the Console Event Log report is the same as the Alarms and Events tab. For more information on using this report, see the "Alarms and Events" Help topic.
- **Wireless** — A collection of summary reports providing information on your wireless network components, including reports for AP groups, APs, clients, controllers, and mobility zones. Wireless reports also provide data on wireless components ranked by bandwidth and clients, such as top APs by bandwidth, top clients by bandwidth, and top controllers by clients, as well as reports on APs and controllers that are down. For convenience, you can also view some of these reports from the Wireless tab.
- **PDF Reports** — Generate summary reports of your current network configuration in PDF format including a Console Report, Network Status Summary, Inventory Report, Identity and Access Summary, and Wireless Configuration Report. You can save these reports or send them to other users in the organization.

Custom Report

Use the **Custom Report** tab to help diagnose a target/statistic pair collection problem as well as view specific ranges of data for a known target. It is a historical report with fully selectable parameters including targets, statistics, category, date range, and display options. Choose the report target such as APs, controllers, or interfaces, as well as the statistics to report on, time frames, and more. Display reports either as a chart or table. You can bookmark the reports you create to view at a later time or to allow you to share the report with others. Report data can also be exported to a file in CSV format. For more information, click the **Info** button ℹ at the top-right of the **Reports** tab.

Report Designer

The Report Designer lets you create custom dashboard reports by selecting from a list of available Application Analytics, IAM, Console, and Wireless dashboards, and customizing report components to meet your specific needs.

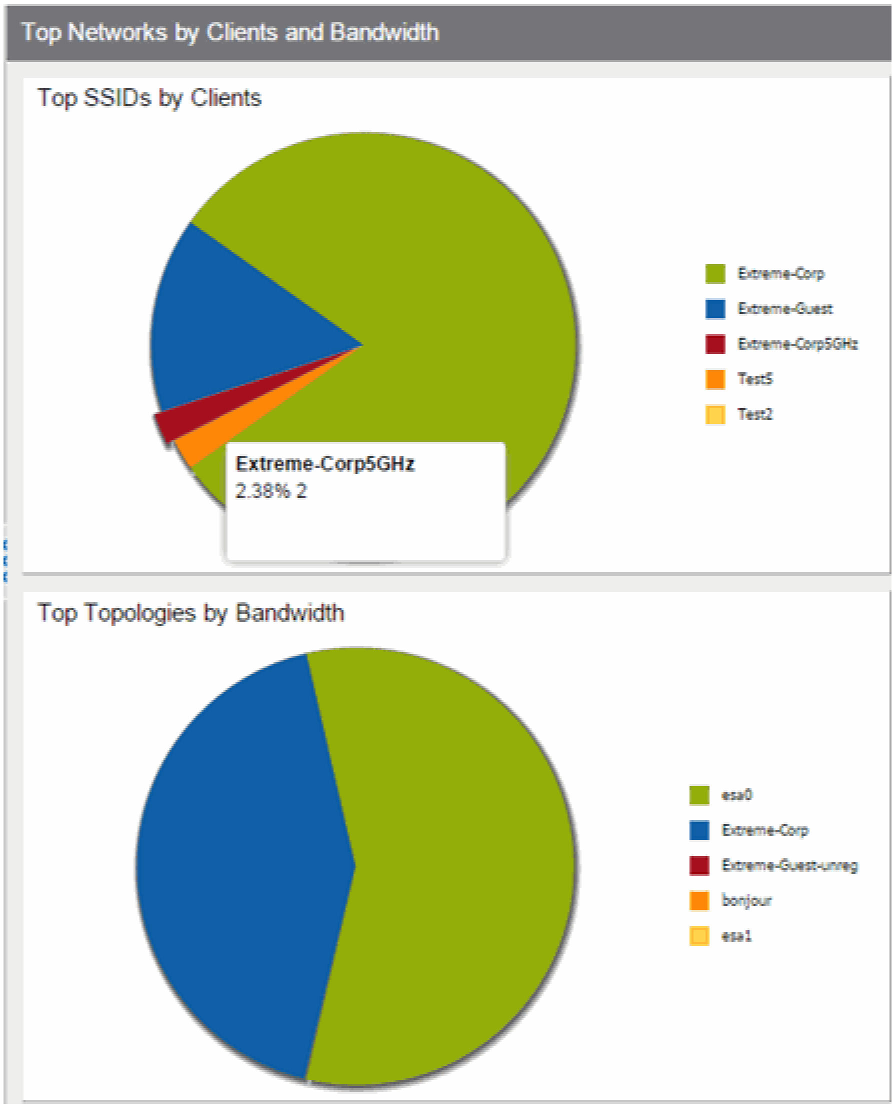
Once a report is created, it is available from the Reports tab.

For instructions on creating a custom report, see How to Use the Report Designer.

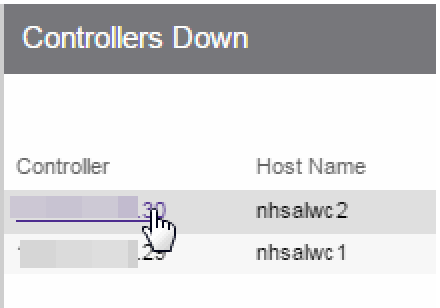
Report Features

Extreme Management Center reports include the following features (depending on the report selected):

- Hover Over for Info — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, clicking on a pie section opens a filtered end-systems grid for more detailed information.



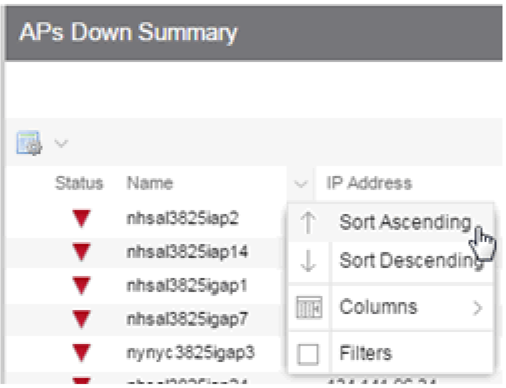
- Drill-down for Details — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



Controllers Down

Controller	Host Name
[redacted].30	nhsalwc2
[redacted].2	nhsalwc1

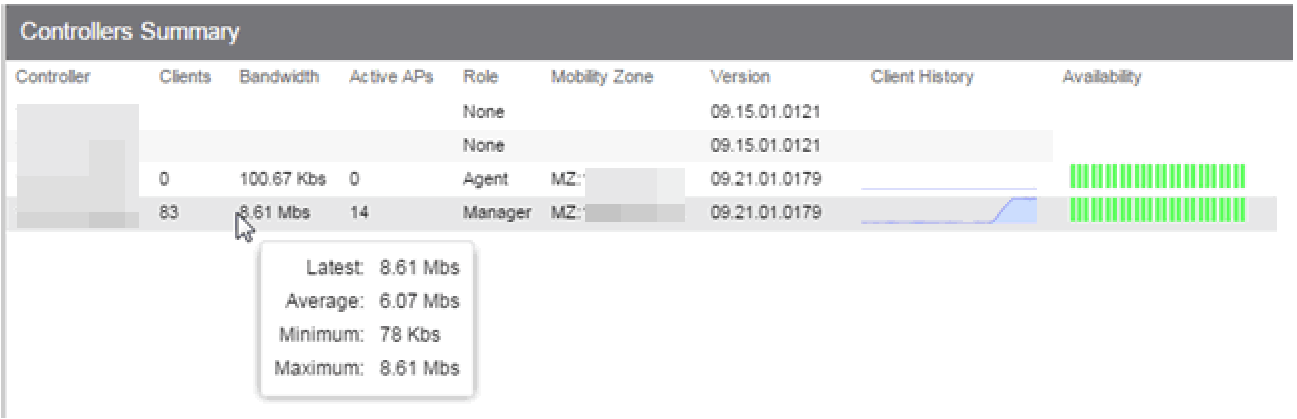
- Interactive Tables — Manipulate table data in several ways to customize the view for your own needs:
    - Click on the column headings to perform an ascending or descending sort on the column data.
    - Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
    - Filter, sort, and search the data in each column in the table.



APs Down Summary

Status	Name	IP Address
▼	nhsal3825iap2	
▼	nhsal3825iap14	
▼	nhsal3825igap1	
▼	nhsal3825igap7	
▼	nynyc3825igap3	

- 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.

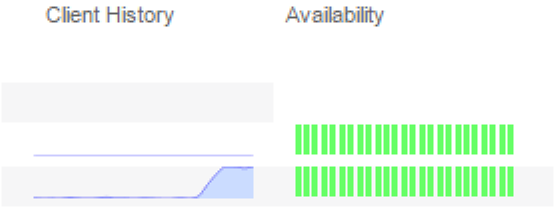


Controllers Summary

Controller	Clients	Bandwidth	Active APs	Role	Mobility Zone	Version	Client History	Availability
[redacted]				None		09.15.01.0121		
[redacted]				None		09.15.01.0121		
[redacted]	0	100.67 Kbs	0	Agent	MZ:[redacted]	09.21.01.0179		
[redacted]	83	8.61 Mbs	14	Manager	MZ:[redacted]	09.21.01.0179		

Latest:	8.61 Mbs
Average:	6.07 Mbs
Minimum:	78 Kbs
Maximum:	8.61 Mbs

- Sparkline Charts — View network trends in dense, succinct charts that present report data in an easy to read, condensed format. This provides you with a quick way to catch possible problem areas that you can investigate further. Rollover charts for additional information.



- CSV Export — Save report data to a file in CSV format to provide report data in table form.

Related Information

For information on related Extreme Management Center tabs:

- Administration
- Alarms and Events
- Network
- Search
- Wireless

The Report Designer lets you create and modify custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The Report Designer also lets you create a new report based on individually selected components, or delete a customized report. Once a report is created, it is available from the report catalog in the **Reports** tab.

The Report Designer can be accessed from the **Reports** tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

Creating a Report

There are two ways to create a report. You can create a report by customizing an existing system report or by creating a new report based on a selection of individual components.

Customize a System Report

Once you change a system report, the new, customized report replaces the original report in the **Reports** tab and all other places in Extreme Management Center where that report is used.

Create a New Report

You can create new reports and add them to your system reports and customized reports on the **Reports** tab. Use the tools in the Report Designer to choose the design and layout, as well as which components are included.

Modifying a Report

You can change a report's components and delete panels, but you cannot add new panels. If you want to add new panels, you must create a new report.

1. Select the **Reports** tab and then select the **Report Designer**.
2. In the My Reports section, select the report you want to modify. The report displays in the right panel for editing.
3. Use the **Component** drop-down menu to change a component in a panel, or click the **Delete** button to delete a panel.
4. Click the **Save** button. The report populates with data and displays in a new tab. This allows you to preview how the customized report looks.

The new report is now listed in the **Reports** tab under the appropriate category.

Deleting a Report

You can delete a customized system report from the My Reports section in the Report Designer. This also deletes the customized report from the **Reports** tab, and replaces it with the original system report. The original report is available again from the System Reports section in the Report Designer.

You can delete a new report from the My Reports section in the Report Designer. This also deletes the new report from the **Reports** tab.

Custom Components

When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the Report Designer to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section of the Report Designer. They are available for selection from the **Component** drop-down menu in the Applications Browser section when you customize a system report or create a new report.

Related Information

- ExtremeAnalytics

Custom Components in

Custom Components

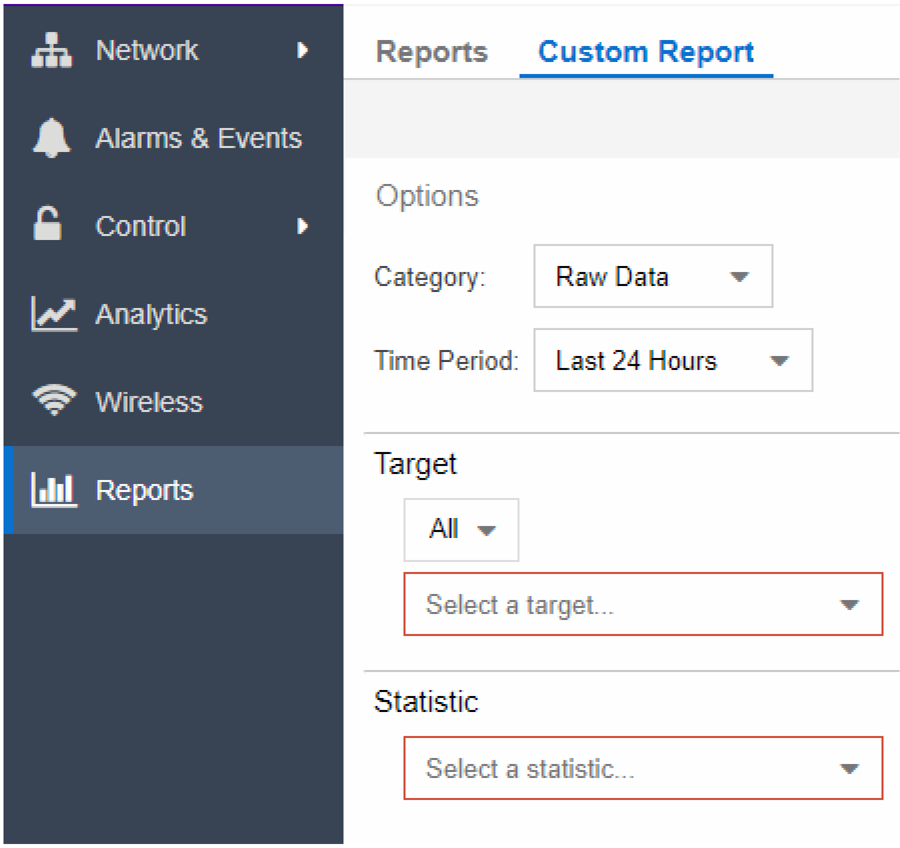
When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the **Report Designer** to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section in the left-panel of the Report Designer. They are available for selection from the **Component** drop-down menu in the Applications Browser section when you customize a system report or create a new report.

Create a New Component

You can create new components from the **Reports > Custom Reports** tab.

The left-panel options allow you to choose the category and duration of the data captured in the component. You can also choose the target for which the data will be displayed, and which statistical data will be displayed.

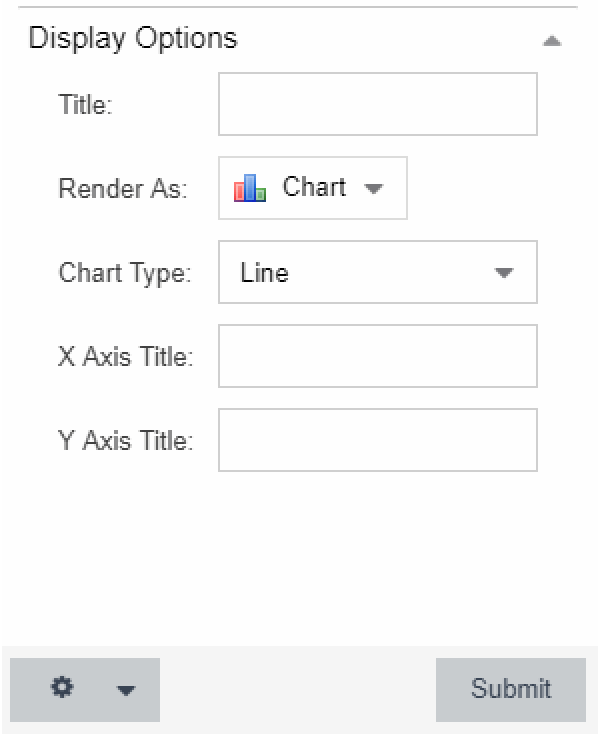


Category: Raw Data

Time Period: Last 24 Hours

All

1. Select a **Category** from the drop-down menu. Options include **Raw Data**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.
2. Choose the **Time Period** for the data to be displayed. Options include **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**, **Last 3 Months**, **Last 6 Months**, **Last Year**, or **Custom**. If you select a custom time period, you can choose your start and end times for the duration of the data.
3. Select the **Target** type from the drop-down menu. Then select the specific target from the **Select a target** drop-down menu.
4. Select the **Statistic** you want to display from the drop-down menu.
5. Enter your **Display Options** to design your chart. You can choose to render the data as a chart or grid.



Display Options

Title:

Render As: Chart

Chart Type: Line

X Axis Title:

Y Axis Title:

6. Click **Submit.**
7. Click the **Gear** button (⚙) in the bottom left corner and choose from the drop-down menu:
   a. (Save) Save to Report Designer - If you choose this option, you can use the component in a new or custom report.
   b. ( ) Export to CSV
   c. ( ) Bookmark
8. Enter a name for your component.

Related Information

For information on related topics:

- Reports

Tasks Overview

The **Tasks** tab in Extreme Management Center allows you to create scripts and workflows and use them to configure tasks. Additionally, you can save a task you run on a device or group of devices, or configure the task to run on a scheduled basis you define.

The **Tasks** tab contains the following sub-tabs:

- Scheduled Tasks
- Scripts
- Workflows
- Saved Tasks
- Task History

Scheduled Tasks

The **Scheduled Tasks** tab allows you to configure Extreme Management Center to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a script
- Email information to Extreme Networks Support
- Discover newly added devices

NOTE: For the email notification to work, configure your SMTP Email Server options. Click the **SMTP** button to open the SMTP Email Server window, where you can define your outgoing email server and the sender's address for your email notifications.

The Scheduled Tasks table lets you view currently scheduled tasks and use toolbar buttons to add, edit, copy, and delete a scheduled task. Click the **Disable** button to disable all active scheduled tasks.

In the table, a green icon (🟢) in the **Status** column indicates the task ran successfully and a red icon (🔴) indicates an error occurred the last time the task ran. Click the red icon for error details.

Click the **Run** button to run a scheduled task immediately without having to change the scheduled run times. This facilitates the testing of scheduled tasks.

Access the event log from the Alarms & Events > **Events** tab, which allows you to display the status of events in Extreme Management Center. Select **Scheduled Task** from the drop-down menu at the top of the table to view task execution events and errors.

Scripts

Extreme Management Center provides you with predefined scripts and allows you to create your own.

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Scripts can be executed on one or more devices or ports, simultaneously on multiple devices or ports, or on one device or port at a time.

You can create tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

Workflows

Workflows you create are modeled as diagrams, with each action linked as a chain. Once you create a workflow, Extreme Management Center performs a complex series of steps with a single click. You can also define a set of actions in the event an action occurs successfully and another set of actions in the event an action does not occur successfully.

Saved Tasks

The Saved Tasks tab allows you to save a script or workflow after running it on a device or group of devices. This allows you configure a task, which can then be run repeatedly on an ad hoc basis.

Task History

The **Task History** tab provides a list of tasks previously run.

The tab also displays the script or workflow running as a result of executing the task and gives additional details about the status of the task.

Related Information

For information on related tabs:

- Workflows
- Saved Tasks
- Scripts
- Scheduled Tasks
- Scripts
- Workflows

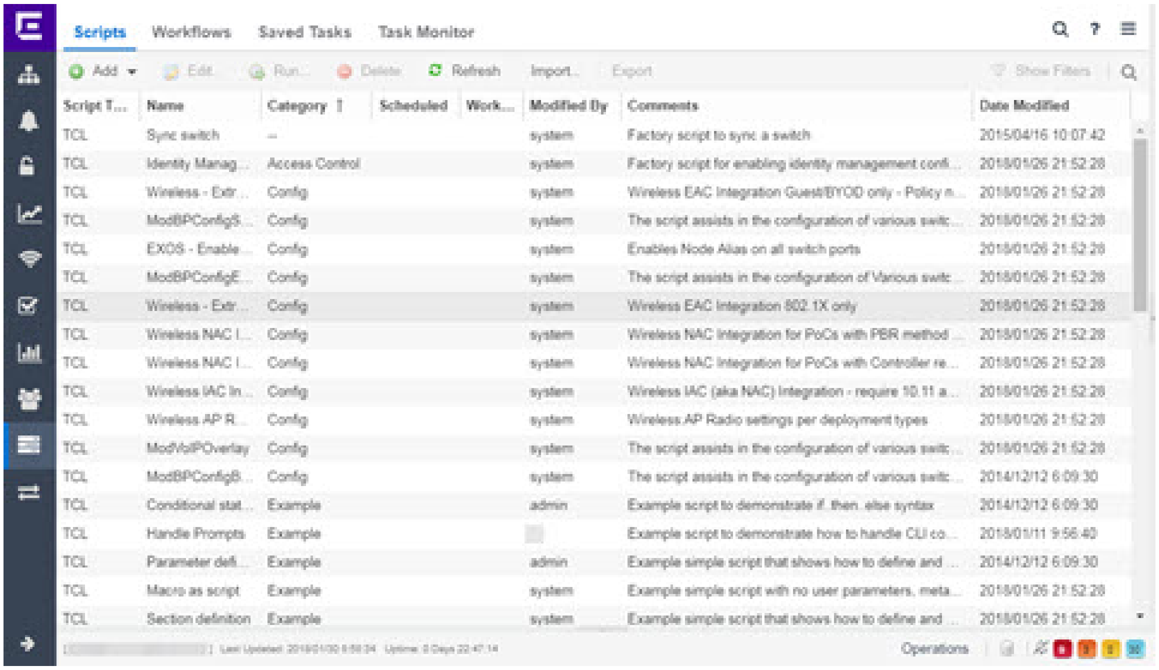
Scripts Overview

Scripting functionality is built into Extreme Management Center, which provides you with predefined scripts and allows you to create your own.

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

You can create tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

To display the scripts configured in Extreme Management Center, open Tasks > Scripts.



Script T...	Name	Category	Scheduled	Work...	Modified By	Comments	Date Modified
TCL	Sync switch	--			system	Factory script to sync a switch	2015/04/16 10:07:42
TCL	Identity Manag...	Access Control			system	Factory script for enabling identity management confi...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration Guest/BYOD only - Policy n...	2018/01/26 21:52:28
TCL	ModBPConfigS...	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	EXOS - Enable...	Config			system	Enables Node Alias on all switch ports	2018/01/26 21:52:28
TCL	ModBPConfigE...	Config			system	The script assists in the configuration of Various switc...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration 802.1X only	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with PBR method ...	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with Controller re...	2018/01/26 21:52:28
TCL	Wireless IAC In...	Config			system	Wireless IAC (aka NAC) Integration - require 10.11 a...	2018/01/26 21:52:28
TCL	Wireless AP R...	Config			system	Wireless AP Radio settings per deployment types	2018/01/26 21:52:28
TCL	ModVoIPOverlay	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	ModBPConfigB...	Config			system	The script assists in the configuration of various switc...	2014/12/12 6:09:30
TCL	Conditional stat...	Example			admin	Example script to demonstrate if..then..else syntax	2014/12/12 6:09:30
TCL	Handle Prompts	Example				Example script to demonstrate how to handle CLI co...	2018/01/11 9:56:40
TCL	Parameter defi...	Example			admin	Example simple script that shows how to define and ...	2014/12/12 6:09:30
TCL	Macro as script	Example			system	Example simple script with no user parameters, meta...	2018/01/26 21:52:28
TCL	Section definition	Example			system	Example simple script that shows how to define and ...	2018/01/26 21:52:28

Last Updated: 2018/01/30 8:58:34 Uptime: 0 Days 22:47:14

Script Type

The language in which the script is written.

Name

The name of the script. The script **Name** is defined when adding the script and can not be edited.

Category

The script category, if configured. The **Category** indicates the purpose of the script.

Scheduled

A checkmark in this column indicates the task is performed on a scheduled basis.

Workflow

A checkmark in this column indicates the task is included in a workflow.

Modified By

The name of the last user to modify the script.

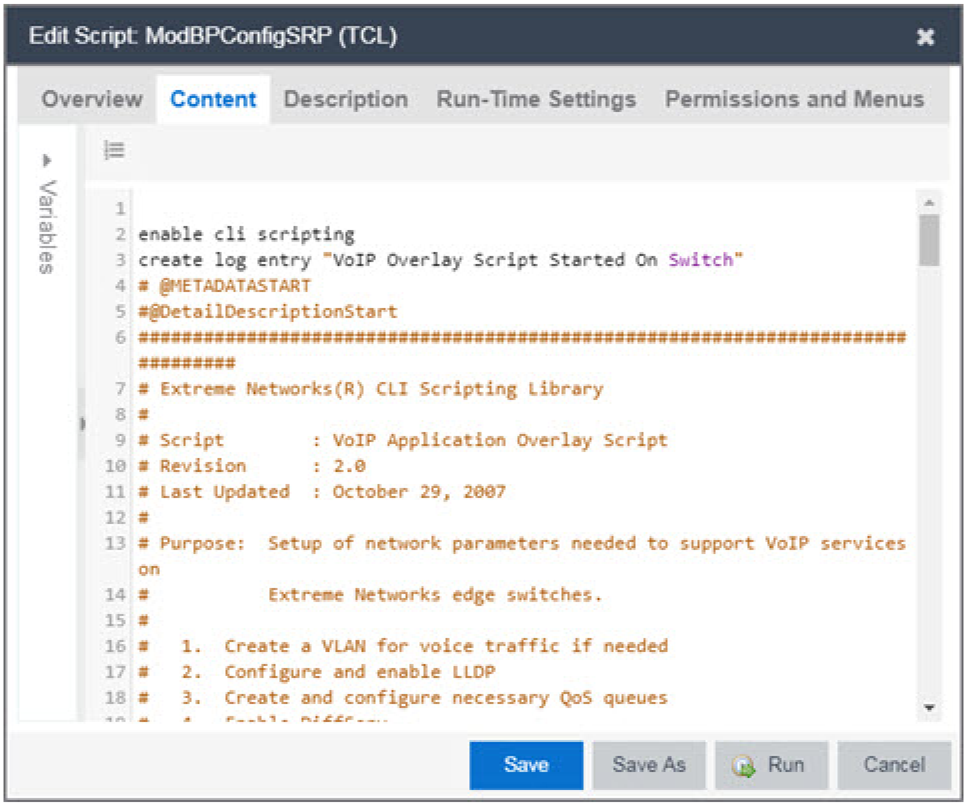
Comments

Comments or a description of the script.

Date Modified

The date the script was last modified.

Double-click a script to open the script editor dialog.



```

enable cli scripting
create log entry "VoIP Overlay Script Started On Switch"
# @METADATASTART
#@DetailDescriptionStart
#######################################################################
#########
# Extreme Networks(R) CLI Scripting Library
#
# Script        : VoIP Application Overlay Script
# Revision      : 2.0
# Last Updated  : October 29, 2007
#
# Purpose:  Setup of network parameters needed to support VoIP services
on
#           Extreme Networks edge switches.
#
#   1.  Create a VLAN for voice traffic if needed
#   2.  Configure and enable LLDP
#   3.  Create and configure necessary QoS queues
```

Related Information

For information on related tabs:

- How to Create Scripts in Extreme Management Center
- Scheduler

How to Create Scripts

This chapter describes the scripting functionality built into Extreme Management Center, and how to use Extreme Management Center to create scripts.

Extreme Management Center Script Overview

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Extreme Management Center scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

Extreme Management Center allows you to create Extreme Management Center tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

Extreme Management Center scripts are similar to ExtremeXOS scripts in that they are collections of ExtremeXOS CLI commands and control structures. Extreme Management Center scripts add some additional commands specific to Extreme Management Center.

In general, Extreme Management Center scripts support syntax and constructs from the following sources:

- ExtremeXOS CLI commands — ExtremeXOS CLI commands in a Extreme Management Center script are sent to the device or port and the response can be used by the script. Abbreviated ExtremeXOS commands do not work unless you prefix the shortened command with CLI. For example, to abbreviate show vlan, type `CLI sh vlan`.
- ExtremeXOS CLI scripts — Control structures such as IF..ELSE and DO..WHILE can be used in Extreme Management Center scripts. See "CLI Scripting" in the *ExtremeXOS User Guide* for more information on ExtremeXOS script functionality and syntax.
- 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 Extreme Management Center scripts, see "Tcl Support in Extreme Management Center Scripts".

  Syntax and constructs from these sources work seamlessly within Extreme Management Center scripts. For example, the response from a switch to an ExtremeXOS CLI command issued from a script can be processed using Tcl functions.

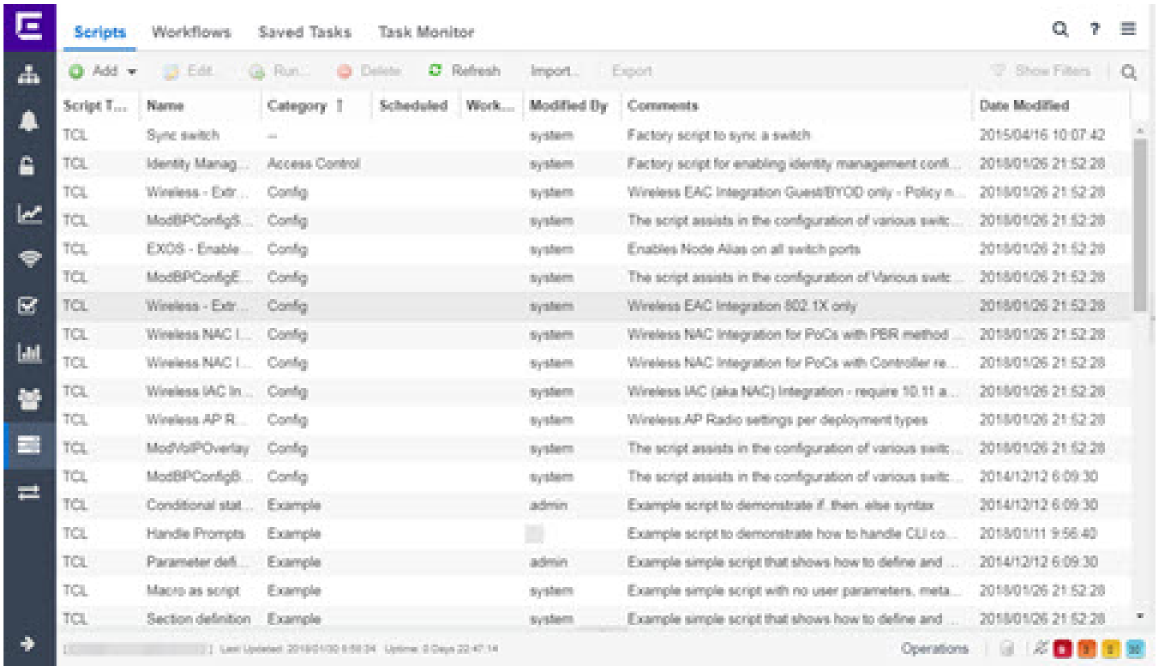
Bundled Extreme Management Center Scripts

Extreme Management Center includes a number of sample scripts you can use as templates for your own Extreme Management Center scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with Extreme Management Center are available to users with an Administrator role. The XML source files for the scripts are located at `<install directory>\appdata\scripting\bundled_scripts`.

The Extreme Management Center Script Interface

To display the scripts configured in Extreme Management Center, select the **Tasks** tab, then click the **Scripts** subtab.



Script T...	Name	Category	Scheduled	Work...	Modified By	Comments	Date Modified
TCL	Sync switch	--			system	Factory script to sync a switch	2015/04/16 10:07:42
TCL	Identity Manag...	Access Control			system	Factory script for enabling identity management confi...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration Guest/BYOD only - Policy n...	2018/01/26 21:52:28
TCL	ModBPConfigS...	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	EXOS - Enable...	Config			system	Enables Node Alias on all switch ports	2018/01/26 21:52:28
TCL	ModBPConfigE...	Config			system	The script assists in the configuration of Various switc...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration 802.1X only	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with PBR method...	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with Controller re...	2018/01/26 21:52:28
TCL	Wireless IAC In...	Config			system	Wireless IAC (aka NAC) Integration - require 10.11 a...	2018/01/26 21:52:28
TCL	Wireless AP R...	Config			system	Wireless AP Radio settings per deployment types	2018/01/26 21:52:28
TCL	ModVoIPOverlay	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	ModBPConfigB...	Config			system	The script assists in the configuration of various switc...	2014/12/12 6:09:30
TCL	Conditional stat...	Example			admin	Example script to demonstrate if..then..else syntax	2014/12/12 6:09:30
TCL	Handle Prompts	Example				Example script to demonstrate how to handle CLI co...	2018/01/11 9:56:40
TCL	Parameter defi...	Example			admin	Example simple script that shows how to define and ...	2014/12/12 6:09:30
TCL	Macro as script	Example			system	Example simple script with no user parameters, meta...	2018/01/26 21:52:28
TCL	Section definition	Example			system	Example simple script that shows how to define and ...	2018/01/26 21:52:28

Last Updated: 2018/01/30 8:58:34 Uptime: 0 Days 22:47:14

The **Scripts** tab contains the following information:

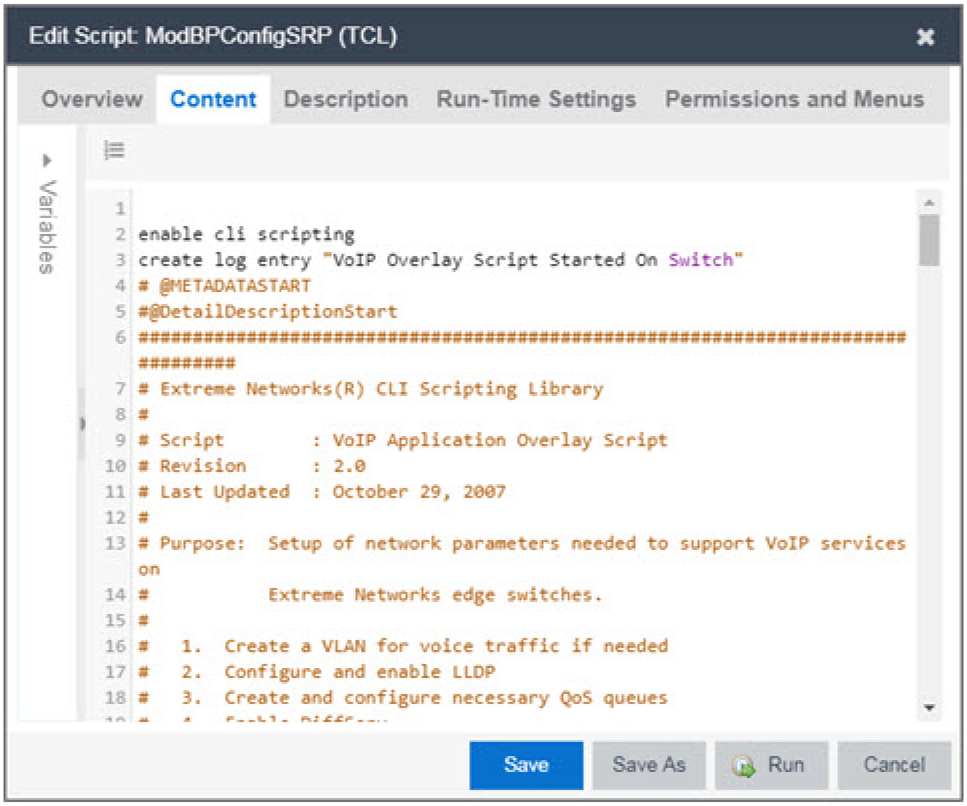
- **Category** — The script category, if configured.
- **Task** — Indicates whether the script is used in a scheduled task.
- **Name** — The name of the script.
- **Comments** — Comments or a description of the script.
- **Modified By** — The name of the last user to modify the script.
- **Date Modified** — The date the script was last modified.

The **Saved 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 saved task.
- **User Name** — The name of the last user to modify the saved task.
- **Script Name** — The name of the script run by the script task.
- **Comment** — Comments or a description of the script task.
- **Date Modified** — The date the script task was last modified.

Double-click a script to open the script editor dialog.



```

enable cli scripting
create log entry "VoIP Overlay Script Started On Switch"
# @METADATASTART
#@DetailDescriptionStart
################################################################################
# Extreme Networks(R) CLI Scripting Library
#
# Script        : VoIP Application Overlay Script
# Revision      : 2.0
# Last Updated  : October 29, 2007
#
# Purpose:  Setup of network parameters needed to support VoIP services on
#           Extreme Networks edge switches.
#
#   1.  Create a VLAN for voice traffic if needed
#   2.  Configure and enable LLDP
#   3.  Create and configure necessary QoS queues
#   4.  Enable DiffServ
```

The Extreme Management Center script editor allows you to add content to a script, set values for parameters, specify run-time settings, and indicate the Extreme Management Center users that can run the script.

The following tabs appear in the Extreme Management Center **Script Editor** window:

- **Overview** — Displays fields to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
- **Content** — Displays the script in a text editor window, where you can modify it directly.

- **Description** — Contains descriptive information about the script. The script description is specified in the metadata section of the script.
- **Run-Time Settings** — Specifies script settings applied when the script is run.
- **Permissions and Menus** — Specifies Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.

Managing Extreme Management Center Scripts

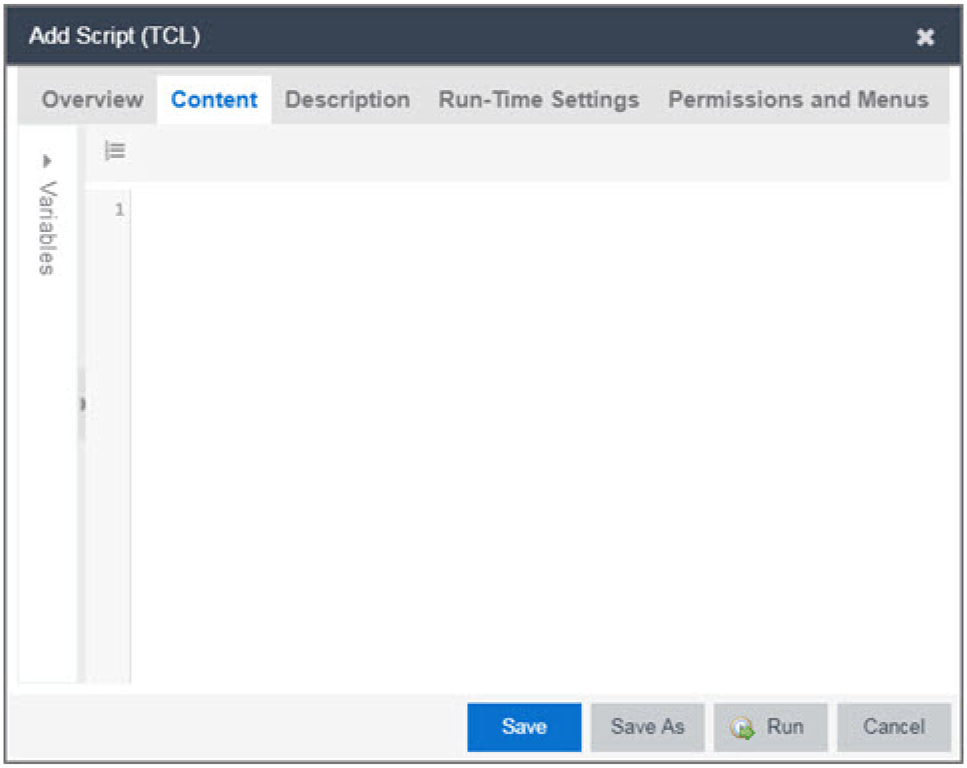
With scripting, you can:

- Create an Extreme Management Center Script
- Specify Run-Time Settings for a Script
- Specify Permissions and Run Locations for Scripts
- Run a Script
- View Script Results
- Edit a Script
- Delete a Script
- Import Scripts into Extreme Management Center
- Export a Script
- Configure Script Tasks

Create an Extreme Management Center Script

1. On the **Tasks** tab, click **Scripts**.
2. Click the **Add** button and select the type of script you are creating:
3. Select the type of script you are creating:
    - **TCL** — Tool Command Language
    - **Python** — Python script
    - **JSON-RPC-CLI** — Machine to Machine Interface (used to send CLI commands to an ExtremeXOS device).
    - **JSON-RPC-Python** — Machine to Machine Interface (used to send a Python script to an ExtremeXOS device).

4. The Add Script dialog box appears.



5. 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.
6. Place variable definition statements in the metadata section (between `#@MetaDataStart` and `#@MetaDataEnd` tags).

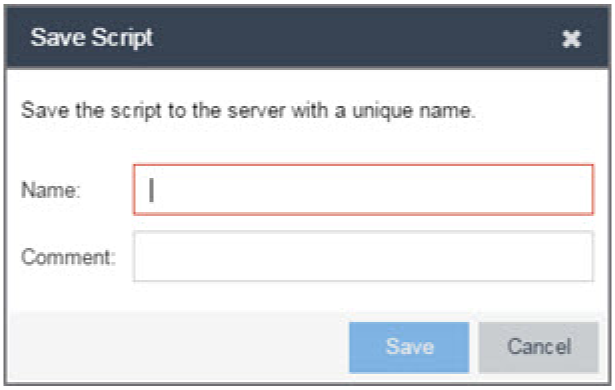
   Variables can be defined by expanding the Variables menu on the left of the **Content** tab. A list of system variables appears under Variables. To add a variable to the script, double-click the variable.
7. Enter the script commands after the metadata section of the script. For information about what can appear in a Extreme Management Center script, see Extreme Management Center Script Reference.

   The following are examples of valid script commands:

   - ExtremeXOS 12.1 and later CLI scripting commands
   - TCL commands

- Constructs

8. Click the **Run-Time Settings** tab and make changes as need if you want to specify run-time settings. For additional information, see Specifying Run-Time Settings for a Script.
9. To specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu, click the **Permissions And Menus** tab and make changes as needed. For additional information, see Specifying Permissions and Run Locations for Scripts.
10. Click **Save**. The Save Script dialog box appears.


Save Script

Save the script to the server with a unique name.

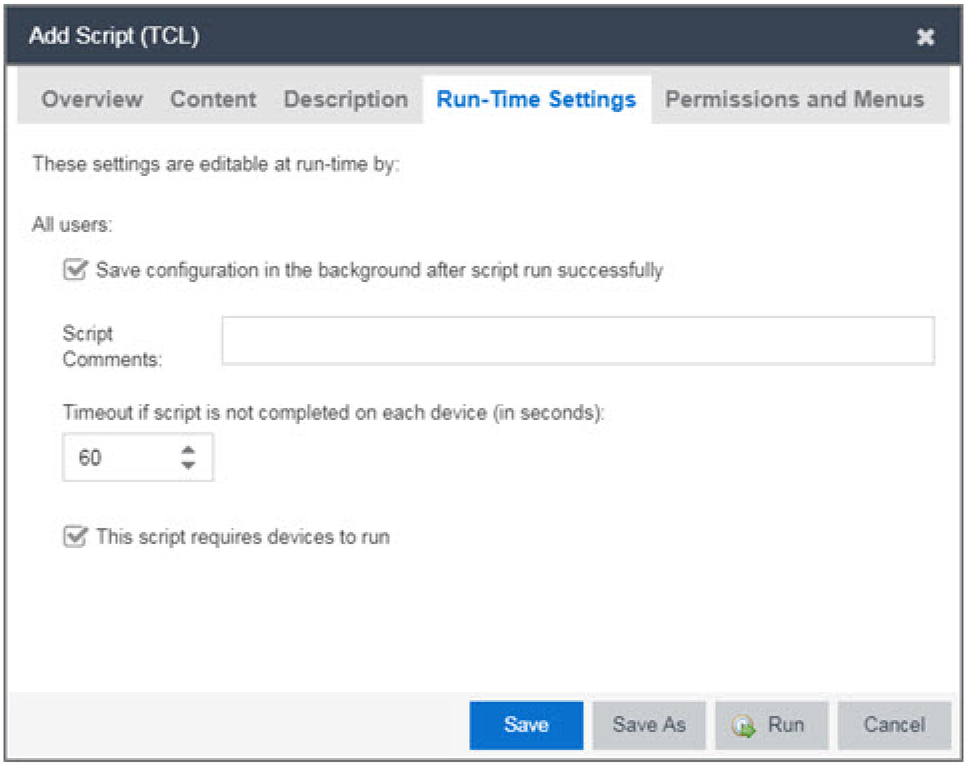
Name:

Comment:

11. 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.
12. Click **Save**.
13. Click **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Run-Time Settings for a Script

To specify the run-time settings for a script, click the **Run-Time Settings** tab.



These settings are editable at run-time by:

All users:

☑ Save configuration in the background after script run successfully

Script Comments:

Timeout if script is not completed on each device (in seconds): 60

☑ This script requires devices to run

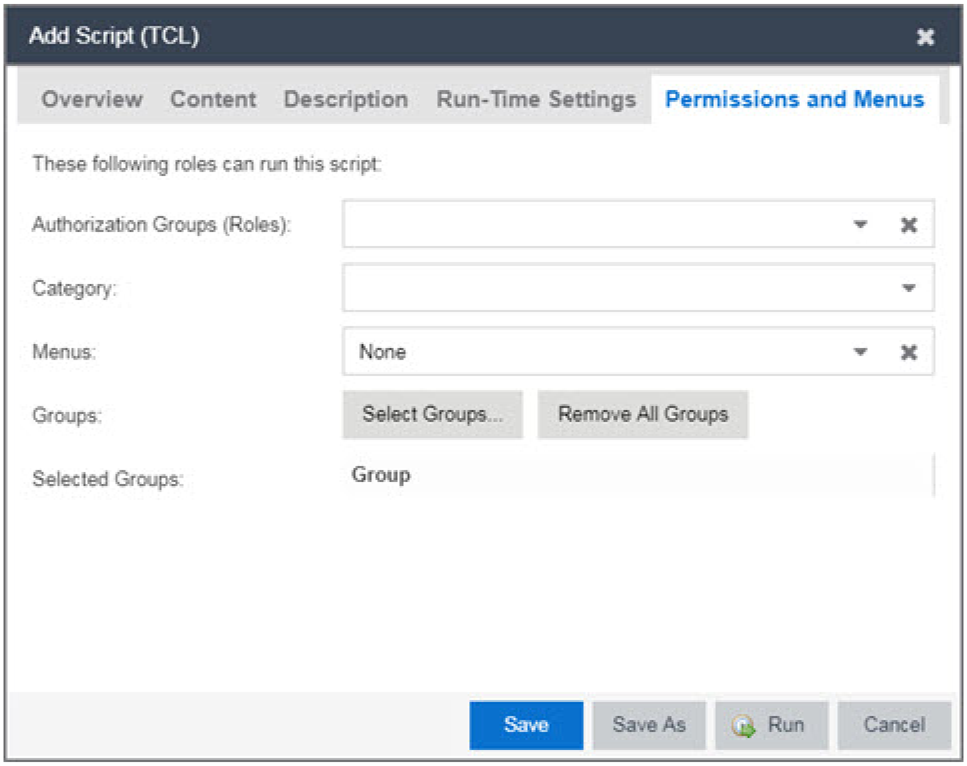
Use this tab to specify the following settings:

- **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 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 or port (in seconds). This timeout value applies to each device or port independently.

Specify Permissions and Run Locations for Scripts

Specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.

Click the **Permissions and Menus** tab to set permissions and menu locations for the script.


Add Script (TCL)

These following roles can run this script:

Authorization Groups (Roles):

Category:

Menus: None

Groups:

Selected Groups: Group

- Specify the Extreme Management Center user roles able to see and run the script. Select the check boxes for the roles you wish to enable.
- Set if and where the script appears in the menu and in a shortcut menu in the given locations.

Run 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 devices and to control the order of the selected devices.
4. Click **Next**.
5. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, click the **Description** tab to view the description defined for the script.
6. Click **Next**.

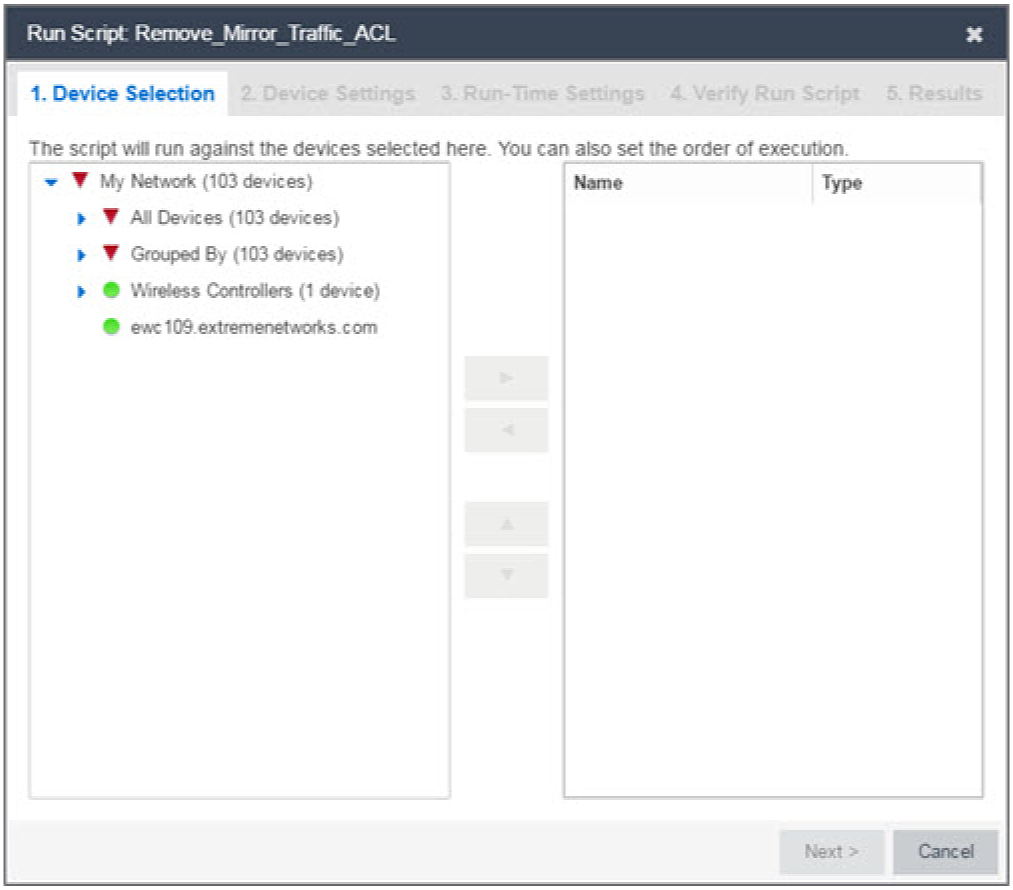
7. On the **Run-Time Settings** tab, set the run-time settings for the script. For additional information, see Specifying Run-Time Settings for a Script.
   - **Save configuration in the background after script run successfully** — When selected, the configuration on the device is saved after the script 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 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 Create Script Tasks.
   - **Save as a 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 Create 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 Tasks tab:

1. Click **Scripts**.
2. On the **Scripts** tab, find the script in the list. If needed, filter the list by typing search terms in the search box.
3. Select the script by clicking its row and then click **Run**. The Run Script window opens.

NOTE: Be sure to select only one script. The **Run** button is unavailable if two or more scripts are selected.

4. On the **Device Selection** tab, shown below, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the selected devices.



Run Script: Remove_Mirror_Traffic_ACL

The script will run against the devices selected here. You can also set the order of execution.

My Network (103 devices)
All Devices (103 devices)
Grouped By (103 devices)
Wireless Controllers (1 device)
ewc109.extremenetworks.com
Name
Type
Next >
Cancel

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 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 Create Script Tasks.
   - **Save as a 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 Create 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**.

View Script Results

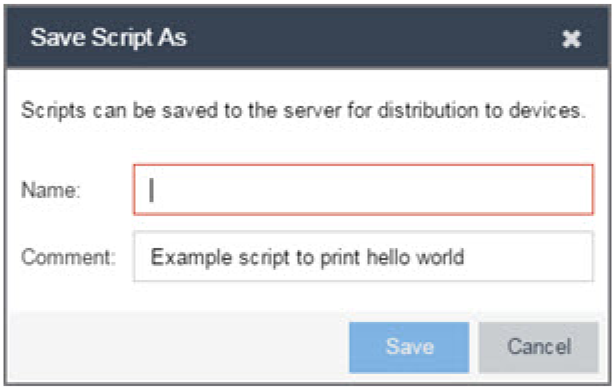
Once a script is run, results are stored in the `<install directory>/appdata/scripting/tmp` folder. The folder in which script results are stored cannot be configured.

An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. Once the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select the script you want to edit.
3. Click the **Edit** button. The script opens in the Edit Script window, where you can edit the script.
4. Click **Save As**. The **Save Script As** dialog box appears.



Save Script As

Scripts can be saved to the server for distribution to devices.

Name: |

Comment: Example script to print hello world

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.

Delete a Script

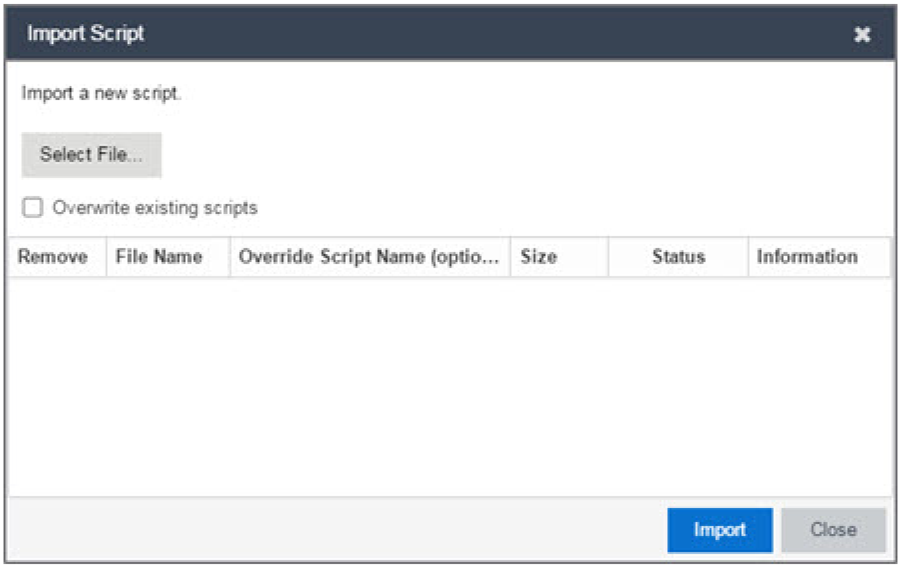
To delete a script:

1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the script deletion.

Import Scripts into Extreme Management Center

Import XML-formatted scripts into Extreme Management Center. To import a script:

1. In the **Tasks** tab, click **Scripts**.
2. Click the **Import** button.



Import a new script.

☐ Overwrite existing scripts

Remove	File Name	Override Script Name (optio...	Size	Status	Information

3. Click **Select File** to navigate to the location of the script. The script appears in the grid.
4. Enter a new Script Name in the Override Script Name (optional) field if you want to edit the name of the script.
5. Click **Import**.
6. Verify the script is imported and click **Close**.

NOTE: Exported EPICenter 6.0 telnet macros cannot be imported as XML scripts.

Export a Script

To export a script:

1. From the **Tasks** tab, select a script.
2. Click the **Export** button.

The script is exported in XML format to your browser download directory.

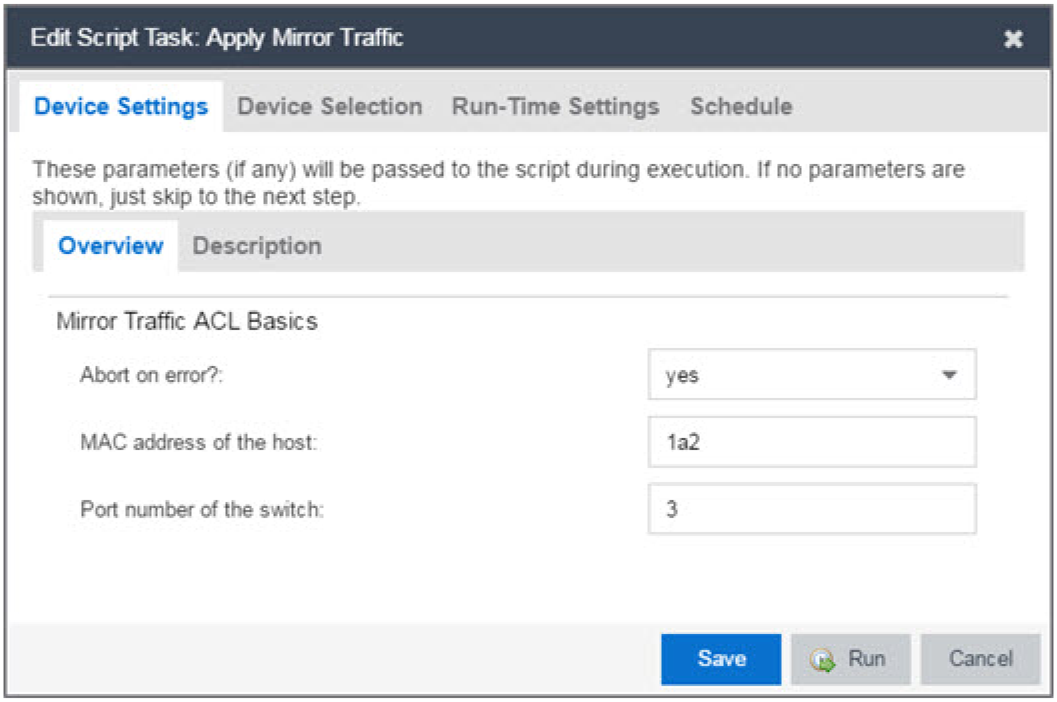
Configure Script Tasks

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 a regular basis.

Create Saved Tasks

To create a saved task, you need to:

1. Select a script or workflow.
2. Run the script or workflow and designate it as a task by selecting either **Save as a task and run now** or **Save as task. I'll run later** on the **Run-Time Settings** tab.
3. Click the **Saved Tasks** tab.
4. Double-click the saved task or click the saved task and click **Open**. The Edit Saved Task window appears (see the following figure).



These parameters (if any) will be passed to the script during execution. If no parameters are shown, just skip to the next step.

Mirror Traffic ACL Basics

Abort on error?: yes

MAC address of the host: 1a2

Port number of the switch: 3

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 on the **Schedule** tab to schedule the script task to run automatically.
   a. Click the **Schedule Task** button.
   b. Select the script task you want to run in the **Saved Task Name** drop-down menu.

c. Enter a **Task Name** and **Description** for the scheduled task in the Task Details section.

d. Select how often you want the scheduled task to run in the Recurrence Pattern section.

e. Select the starting and ending date and time to run the script task using the **Start** and **End** date and time fields in the Date/Time Range section of the window.

f. Enter the scheduled task recipient's email address in the **To** field and enter any information you want to include in the email when the scheduled task is sent in the **Subject** and **Body** fields.

g. Click **Save**.

The saved task is now scheduled to run automatically on the date and time you configured.

8. Click **Save** to save any changes.
9. Click **Run** to run the saved task or **Cancel** to exit the script task.

Deleting Saved Tasks

If desired, delete saved tasks you no longer need. To delete a saved task:

1. Remove any schedules configured (Scheduled = Recurring or One-time) with the saved task by clicking the **Saved Tasks** tab, selecting the associated schedule, and clicking **Delete**.
2. Select the **Tasks** tab, click the **Saved Tasks** tab.
3. Select the saved task in the table.
4. Click the **Delete** button.

Extreme Management Center Script Reference

This section contains reference information for Extreme Management Center scripts. It contains the following topics:

- Metadata Tags
- Extreme Management Center-Specific Scripting Constructs
- Tcl Support in Extreme Management Center Scripts
- Entering Special Characters

- Line Continuation Character
- Case Sensitivity in Extreme Management Center Scripts
- Reserved Words in Extreme Management Center Scripts
- ExtremeXOS CLI Scripting Commands Supported in Extreme Management Center Scripts
- Extreme Management Center-Specific System Variables

A Extreme Management Center script may contain a metadata section, which can serve as a usability aid in the script interface. The metadata section, if present, is the first section of a Extreme Management Center script, followed by the script logic section, which contains the CLI commands and control structures in the script. The metadata section is delimited between `#@MetaDataStart` and `#@MetaDataEnd` tags. A metadata section is optional in a Extreme Management Center script.

Use metadata tags to specify the description of the script, as well as parameters that the script user can input. The information specified by the metadata tags appears in the **Overview** tab for the script.

Metadata Tags

#@MetaDataStart and #@MetaDataEnd

Indicates the beginning and end of the metadata section of the script. In order for description information and variable input fields to appear in the **Overview** tab for a script, the corresponding metadata tags must appear in the metadata section.

Example

```
#@MetaDataStart

#@SectionStart (description = "Protocol Configuration
Section") Set var protocolSelection eaps

#@SectionEnd

#@SectionStart (description = "vlan tag section") Set var
vlanTag 100

#@MetaDataEnd
```

#@ScriptDescription

Specifies a one-line description of the script. The description specified with this tag cannot contain a newline character.

Example

```
#@ScriptDescription "This is a VLAN configuration script."
```

#@DetailDescriptionStart and #@DetailDescriptionEnd

Specifies the beginning and end of the detailed description of the script. The detailed description can be multiple lines or multiple paragraphs. The detailed description is shown in the **Script View** tab in the script editor window.

Example

```
#@DetailDescriptionStart

#This script performs configuration upload from Extreme
Management Center to the switch.

#The script only supports tftp.

#This script does not support third party devices.

#@DetailDescriptionEnd
```

#@SectionStart and #@SectionEnd

Specifies the beginning and end of a section within the metadata part of a script. 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 Extreme Management Center:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response

- Synchronizing the Device with Extreme Management Center
- Saving the Configuration on the Device Automatically
- Printing a String to the Output File

Specifying the Wait Time Between Commands

After the script executes a command, the sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
sleep 5
```

Example

```
# sleep for 5 seconds after executing a command

sleep 5
```

Printing System Variables

The printSystemVariables command prints the current values of the system variables. Specifically, values for the following variables are printed:

- deviceIP
- deviceName
- serverName
- deviceSoftwareVer
- serverIP
- serverPort
- date
- time
- abort_on_error
- CLI.OUT

Syntax

```
printSystemVariables
```

Example

```
# Display values for system variables
```

```
printSystemVariables
```

Configuring a Carriage Return Prompt Response

A special string within the script, `<cr>`, indicates a carriage return in response to a prompt for a command.

Syntax

```
<cr>
```

Example

```
# cancel download

download image 10.22.22.22 t.txt <cr>
```

Synchronizing the Device with Extreme Management Center

The PerformSync command manually initiates a synchronization for specified Extreme Management Center feature areas and scope.

Syntax

```
PerformSync [-device <ALL | deviceIp>] [-scope <EAPSDomain |
VPLS> ]
```

If -device is not specified, the current device (indicated by the `$deviceIP` system variable) is assumed.

The PerformSync command is executed in an asynchronous manner so when the command is executed, Extreme Management Center moves on to the next command in the script without waiting for the PerformSync command to complete.

Examples

```
PerformSync -scope VPLS
```

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 Extreme Management Center scripts:

after	concat	for	info	lrange	puts	set	unset
append	continue	foreach	interp	lreplace	read	split	update
array	eof	format	join	lsearch	regexp	string	uplevel
binary	error	gets	lappend	lsort	regsub	subst	upvar
break	eval	global	lindex	namespace	rename	switch	variable
catch	expr	history	linsert	open	return	tell	vwait
clock	fblocked	if	list	package	scan	time	while
close	flush	incr	llength	proc	seek	trace	

See www.tcl.tk/man/tcl8.2.3/TclCmd/contents.htm for syntax descriptions and usage information for these Tcl commands.

Entering Special Characters

In a Extreme 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 Extreme Management Center script.

Line Continuation Character

The line continuation character is not supported in Extreme Management Center scripts. Place each command statement on a single line.

Case Sensitivity in Extreme Management Center Scripts

The commands and constructs in a Extreme Management Center script are not case-sensitive. However, if a command is referenced inside another command, the inner command is case-sensitive. In this instance, the inner command case matches how it appears in the Extreme Management Center documentation.

Example (Usage of the Extreme Management Center command ECHO)

```
echo hi (valid)
```

```
echo [echo hi] (error)
```

```
echo [ECHO hi] (valid)
```

Reserved Words in Extreme Management Center Scripts

The following words cannot be used as variable names in a Extreme Management Center script. They are reserved by Extreme Management Center.

- Names of system variables (see Extreme Management Center-Specific System Variables)
- Names of Extreme Management Center command extensions (see Extreme Management Center-Specific Scripting Constructs)
- Names of ExtremeXOS CLI commands
- Names of Tcl functions

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

Extreme Management Center scripts support the CLI commands in this section.

- $VAREXISTS
- $TCL
- $UPPERCASE
- show var
- delete var
- configure cli mode scripting abort-on-error

$VAREXISTS

- Checks if a given variable is initialized.
- Switch Compatibility — Devices running ExtremeXOS 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given Tcl command. The following constructs support the $TCL command:
- `set var if`
  - while
- See Tcl Support in Extreme Management Center Scripts for a list of supported Tcl commands.
- Switch Compatibility — Devices running ExtremeXOS 11.6 and higher support this command.
- Example — `set var foo $TCL(expr 3+4) if ($TCL(expr 2+2) == 4) then`

$UPPERCASE

- Converts a given string to upper case.
- The following constructs support the $UPPERCASE command:
  - set var
  - if
  - while
- Switch Compatibility — Devices running ExtremeXOS 11.6 and higher support this command.

NOTE: The $UPPERCASE command is deprecated in ExtremeXOS 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $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 Extreme Management Center scripts:

$abort_on_error

Whether the script terminates if a CLI error occurs; 1 aborts on error, 0 continues on error.

$CLI.OUT

The output of the last CLI command.

$CLI.SESSION_TYPE

The type of session for the connection to the device, either Telnet or SSH.

NOTE: Variables with TCL special characters must be enclosed in braces. For example, when using the system variables `$CLI.SESSION_TYPE` and `$CLI.OUT` in a script, they must be entered as `${CLI.SESSION_TYPE}` and `${CLI_OUT}`, respectively.

$date

The current date on the Extreme Management Center server.

$deviceIP

The IP address of the selected device.

$deviceLogin

The name of the login user for the selected device.

$deviceName

The DNS name of the selected device.

$deviceSoftwareVer

The version of ExtremeXOS running on the selected device.

$deviceType

The product type of the selected device.

$netsightUser

The name of the Extreme Management Center user running the script.

$isExos

Indicates whether the device is an ExtremeXOS device. Possible values are True or False.

$port

Selected port numbers, represented as a string. If the script is not associated with a port, this system variable is not supported.

$serverIP

The IP address of the Extreme Management Center server.

$serverName

The host name of the Extreme Management Center server.

$serverPort

The port number used by the Extreme Management Center web server; for example, 8080.

$STATUS
: The execution status of the previously executed ExtremeXOS command: 0 if the command executed successfully, non-zero otherwise.

$time
: The current time on the Extreme Management Center server.

$vendor
: Vendor name of the device; for example, Extreme.

Workflows

Workflows you create are modeled as diagrams, with each action linked as a chain. Once you create a workflow, Extreme Management Centerperforms a complex series of steps with a single click. You can also define a set of actions or workflow that would take place if an action occurs successfully, and another set of actions or workflow to take place if that action does not occur successfully.

Once you create a workflow, you can add it to a task, which runs the workflow on specified devices or ports, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

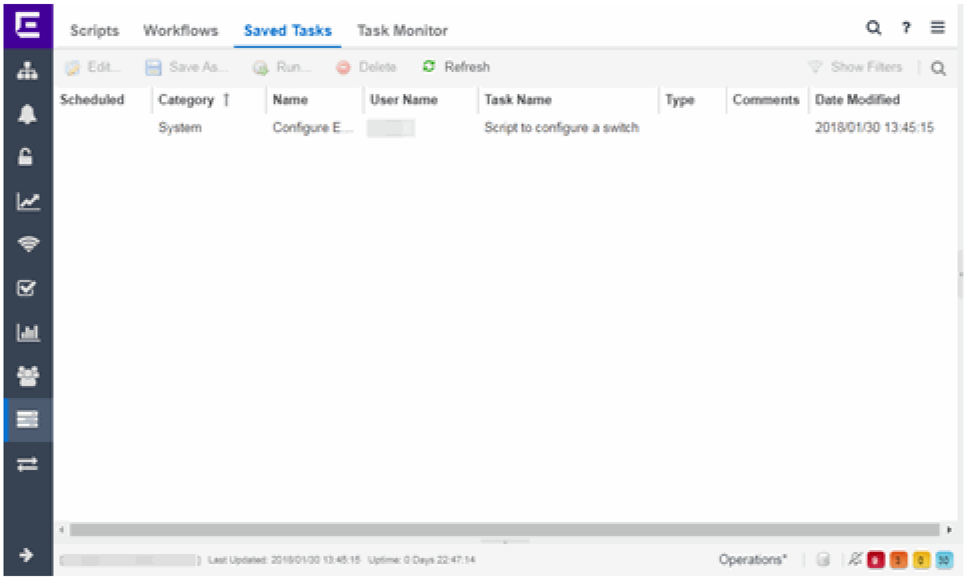
Related Information

For information on related tabs:

- How to Create Scripts in Extreme Management Center
- Scheduler

Saved Tasks

After running a script or workflow on a device or a group of devices, you can save it as a task to run again later. The **Saved Tasks** tab displays the tasks you save for a particular set of devices.



Scheduled	Category	Name	User Name	Task Name	Type	Comments	Date Modified
	System	Configure E...		Script to configure a switch			2018/01/30 13:45:15

Last Updated: 2018/01/30 13:45:15 Uptime: 0 Days 22:47:14

Edit

Click **Edit** to open the **Edit Saved Task** window, where you can edit the task configuration, the devices on which the task is run, and whether the task is automatically run on a scheduled basis.

Save As

Click **Save As** to save the task with a new **Name**, which you can then edit.

Run

Click **Run** to run the task as configured.

Delete

Click **Delete** to remove the task from the **Saved Tasks** tab.

Refresh

Click **Refresh** to update the list of saved tasks.

Scheduled

A checkmark in this column indicates the task is performed on a scheduled basis.

Category

The task category, if configured. **Category** indicates the purpose of the task.

Name

The name assigned to the saved task. The **Name** is defined when saving the script or workflow as a saved task and can not be edited.

User Name

The name of the user who saved the task.

Task Name

The name of the script or workflow running as a result of executing the task. The Task Name is defined when creating the script or workflow and can not be edited.

Workflow

A checkmark in this column indicates the task is included in a workflow.

Comments

Comments or a description of the task.

Date Modified

The date the task was last modified.

Related Information

For information on related tabs:

- How to Create Scripts in Extreme Management Center
- Workflow
- Scheduler

How to Schedule a Task

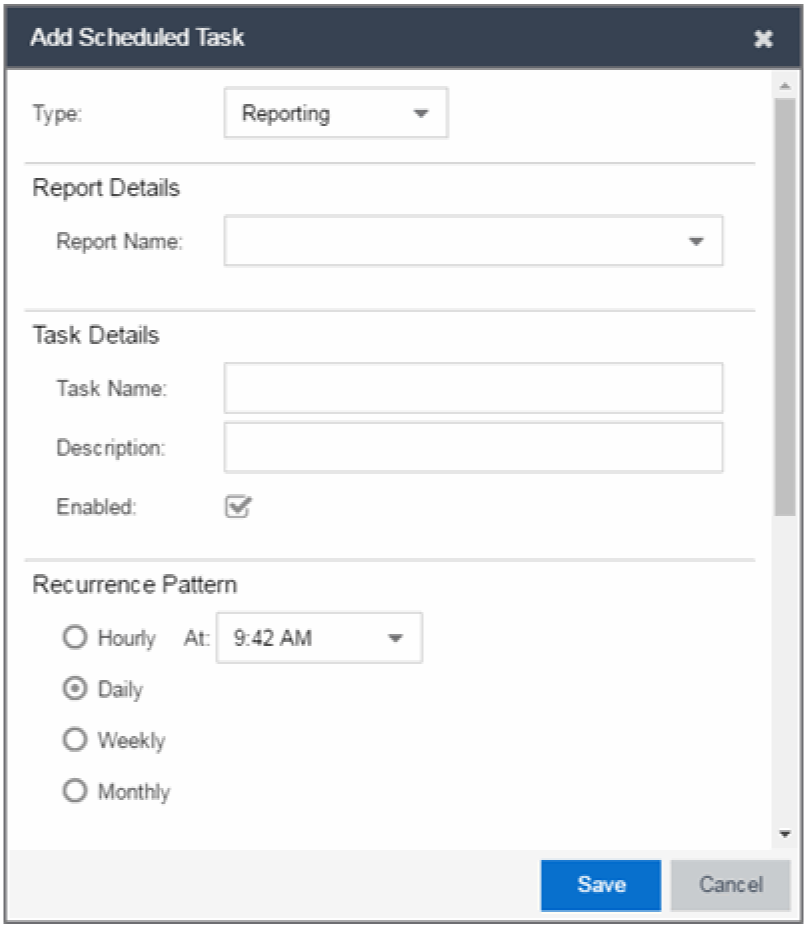
The Scheduled Task tab allows you to configure Extreme Management Center to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a script or workflow
- Email information to Extreme Networks Support
- Discover newly added devices

To create a new task:

1. Launch Extreme Management Center.
2. Select the Tasks tab and select the Scheduled Tasks tab.

3. Click the **Add** button. The Add Scheduled Task window opens.



Add Scheduled Task

Type: Reporting

Report Details

Report Name:

Task Details

Task Name:

Description:

Enabled: ☑

Recurrence Pattern

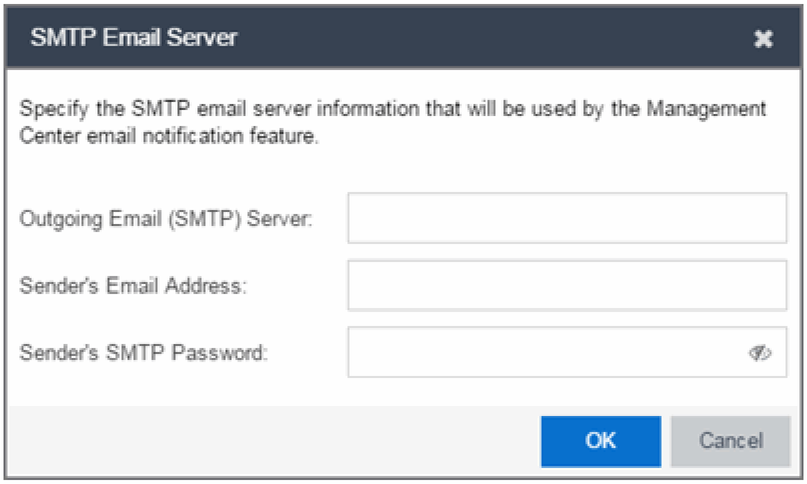
○ Hourly At: 9:42 AM

● Daily

○ Weekly

○ Monthly

If no SMTP email settings are configured, the SMTP Email Server window also opens, where you can define the SMTP email settings. You can also configure the SMTP email settings in the SMTP Email Options tab.



SMTP Email Server

Specify the SMTP email server information that will be used by the Management Center email notification feature.

Outgoing Email (SMTP) Server:

Sender's Email Address:

Sender's SMTP Password:

4. Enter the outgoing SMTP email settings, if necessary, and click **OK**.
5. Select the type of task from the **Type** drop-down menu in the Add Scheduled Task window:
   - **Reporting** — Emails a report you select (created on the Report Designer tab) on a scheduled basis.
   - **Saved Task** — Runs a task saved on the Saved Tasks tab and sends an email on a scheduled basis.
   - **Support** — Emails debugging data on a scheduled basis that provides information to Extreme Networks Support in the event of an issue with your network. *Only select this option if instructed to do so by Extreme Networks Support.*
   - **Site** — Runs a device discover for a site (created on the Site tab) on a scheduled basis.
   - **Disable Alarms** — Disables enabled alarms for the amount of time you define on a scheduled basis. Use this task to avoid alarms during times you reserve for network maintenance activity. You can manually ignore enabled alarms on the Alarm Configuration tab.
6. Select the report, saved task, support task, or site you want to schedule in the **Report Name**, **Saved Task Name**, **Support Task Name**, or **Site to Discover** drop-down menu, respectively. Depending on what you select, you may need to make other selections such as specifying the source engine or controller.
7. Edit the task name and description, if desired.
8. Select or deselect the **Enabled** checkbox to enable or disable the task, respectively. A disabled task is not performed.

9. Select whether you want the task to occur on an hourly, daily, weekly, or monthly basis.
    - **Hourly** — specify the minute each hour you want the task performed.
    - **Daily** — specify the time each day you want the task performed.
    - **Weekly** — specify the day or days of the week and the time you want the task performed.
    - **Monthly** — specify the day of the month and the time you want the task performed.
10. Specify a start and end date and time for the task, if desired.
11. Enter the email address or list of email addresses (separated by semicolons) where you want the generated PDF reports sent.
12. Enter the subject line and body text for the email, if desired.
13. Click **Save**. The task appears in the Scheduled Tasks table.

    Additionally, use the toolbar buttons to edit, copy, or delete the task. The **Refresh** button updates the Scheduled Tasks table to display any recent changes. Clicking the **Disable** button causes a task not to run without deleting it from the Scheduled Tasks table.

    Click the **Run** button to run the scheduled task immediately, if desired.

    Click the **SMTP** button to open the SMTP Email Server window to edit your outgoing email options.

Related Information

For information on related topics:

- Tasks
- SMTP Email Options

Administration

Extreme Management Center's **Administration** tab provides diagnostic reports and tools to monitor, maintain, and troubleshoot the application and its components.

Additionally, the **Menu** icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

To view the diagnostic reports and schedules in the **Administration** tab, you must be a member of an authorization group assigned the OneView > Access OneView and OneView > Access OneView Administration capabilities. For additional information about configuring user capabilities, see Users.

This Help topic provides information on the following sub-tabs:

- Profiles
- Users
- Server Information
- Certificates
- Options
- Backup/Restore
- Diagnostics
- Vendor Profiles

Profiles

The **Profiles** tab allows you to establish access to the devices on your network by creating identities used for authentication when performing SNMP queries and sets. Extreme Management Center supports authentication to devices using SNMPv1, SNMPv2 and SNMPv3. When device models are created in the database, you can accept the default profile or assign a specific Profile to describe a set of access Credentials used for authentication at each level of access in the device. (When first installed, Extreme Management Center's default profile uses an SNMPv1 credential that provides Read, Write and Max

Access privileges.) The specific profile used depends on the protocol that is supported in a device and the credentials that are required to be granted access.

Users

The Users tab allows you to create the authorization groups that define the access privileges (called Capabilities) assigned to authenticated users. When a user successfully authenticates, they are assigned membership in an authorization group that grants specific capabilities in the application.

The **Users** tab is also where you define the method used to authenticate users who are attempting to launch Extreme Management Center. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

Server Information

The Server Information tab allows you to view and manage current client connections and Extreme Management Center locks.

Certificates

The **Certificates** tab provides a central location for managing the Extreme Management Center server certificate.

From this tab you can:

- Update the Extreme Management Center server certificate by replacing the server private key and certificate.
- View and change the client trust mode that specifies how Extreme Management Center clients handles a server certificate.
- View and change the server trust mode that specifies how servers handles certificates from other servers.

Options

Extreme Management Center options allow you to configure the behavior of Extreme Management Center. These options apply across all Extreme Management Center applications. In the **Options** tab (**Administration > Options**), the right-panel view changes depending on what you select in the left-panel tree.

Information on the following options:

- Extreme Access Control Options
- Alarm Options
- Alarm/Event Logs and Table Options
- Compass Options
- Database Backup Options
- Event Analyzer Options
- ExtremeNetworks.com Updates Options
- FlexView Options
- Governance Options
- Impact Analysis Options
- Inventory Manager Options
- Extreme Management Center Options
- Extreme Management Center Collector Options
- Extreme Management Center Engine Options
- Extreme Management Center Server Health Options
- Name Resolution Options
- NetFlow Options
- Network Monitor Cache Options
- Policy Options
- SMTP Email Options
- SNMP Options
- Site Options

- Status Polling Options
- Syslog Options
- TopN Collector Options
- Trap Options
- Web Server Options
- Wireless Manager Options

Backup/Restore

The Backup/Restore tab allows you to perform database backups and a restore operation for legacy backups as well as configure the URL and password for the database.

Diagnostics

The **Diagnostics** tab provides three levels of information: Basic, Advanced, and Diagnostic. Use the Level menu at the top-left of the page to select the desired report level.

- **Basic Level** — This level provides basic administrative reports to help you monitor and troubleshoot your network. It provides a Server Licenses report that displays all server licenses and allows you to add a license and allows you to export end system events for a particular date range in a log file.
- **Advanced Level** — This level includes all Basic administrative reports as well as additional Advanced reports with more detailed information for debugging problems. Beta features can also be enabled from the Advanced level. For additional information on beta features, please contact Extreme Networks Support.
- **Diagnostic Level** — This level includes all Basic and Advanced reports as well as access to the following diagnostic actions:
    - **Save Diagnostic Information** — Saves the administrative report data to log files, and the statistic and target information to CSV files, so that you can save and review the information for debugging purposes. The information is saved to <install directory>/appdata/OneView/RptStatus/ as a zip file, with the date as part of the file name. Unzip the file to view the log files and CSV files. You can view the save operation progress in the Server Log report (located on the Administration tab under the Server section). When the Save operation is

complete, an event is sent to the Console Event log with the full path to the diagnostic zip file.

- Diagnostic Levels — Lets you enable different levels of logging for specific Extreme Management Center functionality, and view the debug information in the Server Log report (located on the **Administration** tab under the Server section) or in the <install directory>/appdata/logs/server.log file on the Extreme Management Center Server. By default, error and informational data is logged to the log file, with a new file created each day. You can set the diagnostic level to Verbose to collect additional data that is presented in an easy-to-read format. Note that the Informational and Verbose settings create large log files and may impact system performance.
  - Off — Turns off all diagnostic logging.
  - 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 Extreme Management Center reporting database. This allows you to restart your database, if required for problem resolution. The operation removes all data from the following database tables:
  - rpt_default_raw
  - rpt_default_hour
  - rpt_default_day
  - rpt_default_week
  - rpt_default_month

Vendor Profiles

The Vendor Profiles tab allows you to edit configurations for devices. The configuration you select determines the reports available for the device in its

DeviceView and lets you choose the FlexView filters that apply to the device. You can also enter additional information about the device to help identify it in Extreme Management Center as well as identify the scripts that apply to the device.

Vendor Profiles are a beta feature and are only available by selecting **Enable Beta Features** on the **Administration** > **Diagnostics** tab.

Related Information

For information on the other Extreme Management Center tabs:

- Alarms and Events
- Devices
- Reports
- Wireless

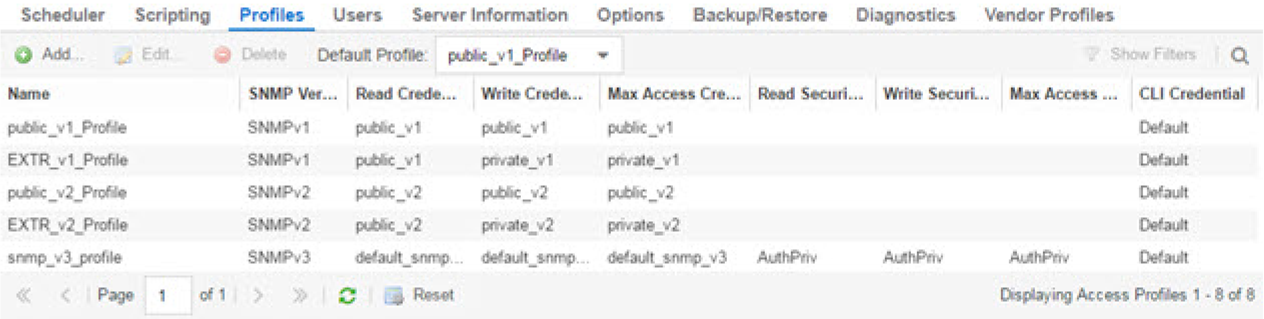
Profiles

Extreme Management Center applications access devices in order to control certain device functions and retrieve information for device properties views, FlexViews and periodic polling. This tab lets you create the authentication *credentials* used to manage access to your devices through SNMP and CLI (command line interface), and the *profiles* that use those credentials for various access levels. Profiles are then mapped to specific devices on your network.

- Credentials — Credentials define the authentication values (for example, user names and passwords) used to access your network devices.
  - SNMP Credentials provide support for device management using SNMP.
  - CLI Credentials provide support for device management using the CLI.
- Profiles — Profiles are assigned to device models in the Extreme Management Center database. They identify the credentials used for the various access levels when communicating with the device.
- Device Mapping — Allows you to map the profiles you create to Authorization Groups on devices.

Managing device access using credentials and profiles consists of creating your credentials, creating the profiles that uses those credentials, and then mapping the profiles to Authorization Groups on devices.

Profiles Section



Default Profile: public_v1_Profile

Name	SNMP Ver...	Read Crede...	Write Crede...	Max Access Cre...	Read Securi...	Write Securi...	Max Access ...	CLI Credential
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1				Default
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2				Default
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default
snmp_v3_profile	SNMPv3	default_snmp...	default_snmp...	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv	Default

Page 1 of 1

Displaying Access Profiles 1 - 8 of 8

Default Profile

This drop-down menu lets you specify a profile used by default to access a device.

ID

This column, hidden by default, displays a unique numeric identifier for the profile.

Name

This is the name assigned when the profile is created. The public_v1_Profile is automatically created during Extreme Management Center installation and cannot be deleted.

SNMP Version

This is the SNMP protocol version for the profile. Profiles can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Read, Write, Max Access Credential

When the Version is SNMPv1 or SNMPv2c, the Read, Write, and Max Access columns in the table contain the Community Name for each access level. When the Version is SNMPv3, the Read, Write, and Max Access columns in the table contain the credential specified for each access level.

Read, Write, Max Access Security Level

When the Version is SNMPv3, these columns contain the security level specified for each access credential. When the Version is SNMPv1 or SNMPv2c, these columns do not apply.

CLI Credential

The CLI credential specified for the profile.

Add Button

Opens the Add/Edit Profile window where you can select the SNMP version and define the profile name and passwords/community names used by the profile.

Edit Button

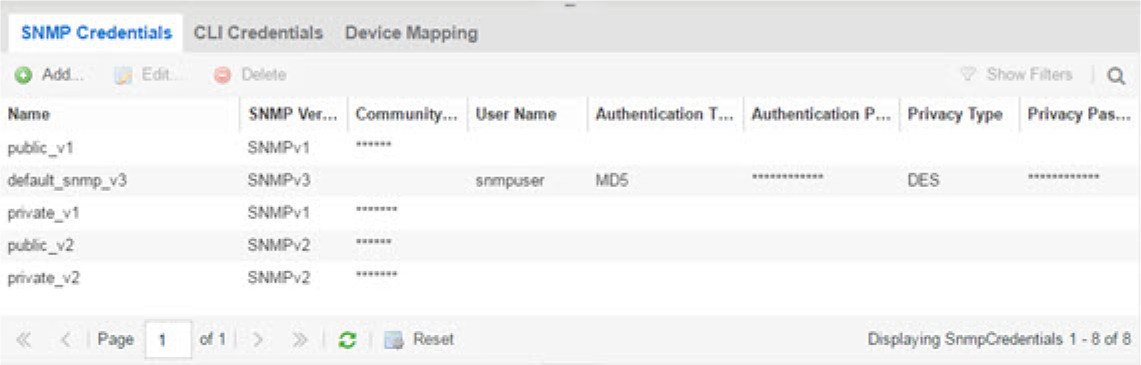
Opens the Add/Edit Profile window where you can modify the SNMP version and passwords/community names used by a selected profile.

Delete Button

Removes the selected Profile from the Device Access Profiles table. You cannot delete the profile currently selected to be the Default Profile.

SNMP Credentials Subtab

This tab lists all of the SNMP credentials created in the Extreme Management Center database. The public_v1 credential is automatically created during installation and cannot be deleted.



Name	SNMP Ver...	Community...	User Name	Authentication T...	Authentication P...	Privacy Type	Privacy Pas...
public_v1	SNMPv1	******					
default_snmp_v3	SNMPv3		snmpuser	MD5	*************	DES	*************
private_v1	SNMPv1	*******					
public_v2	SNMPv2	******					
private_v2	SNMPv2	*******					

Displaying SnmpCredentials 1 - 8 of 8

ID

This column, hidden by default, displays a unique numeric identifier for the SNMP credentials.

Name

This column lists names assigned to credentials created in the Extreme Management Center database.

SNMP Version

This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Community Name

For SNMPv1 or SNMPv2c credentials, this is the Community Name used for device access.

User Name

For SNMPv3 credentials, this is the User Name used for device access.

Authentication Password/Authentication Type, Privacy Password/Privacy Type

For SNMPv3 credentials, these columns show the authentication protocol (None, MD5, or SHA) and privacy protocol (None or DES) and passwords used by the credential.

Add Button

Opens the Add/Edit SNMP Credential window where you can define new SNMP credentials.

Edit Button

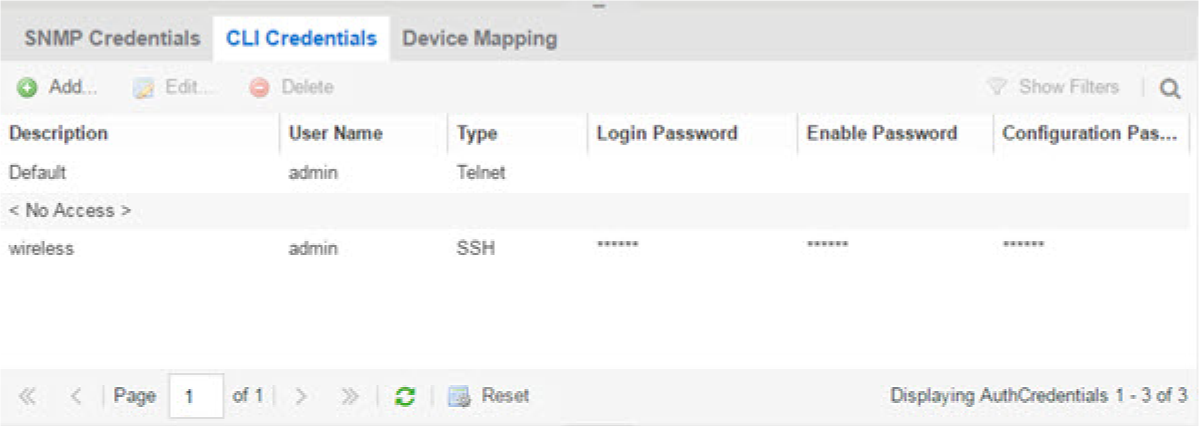
Opens the Add/Edit Credential window where you can modify a credential selected from the SNMP Credentials table.

Delete Button

Removes a selected credential from the SNMP Credentials table.

CLI Credentials Subtab

This tab lists all of the CLI credentials created in the Extreme Management Center database. The Default and <No Access> credentials are created automatically during installation and cannot be deleted.



Description	User Name	Type	Login Password	Enable Password	Configuration Pas...
Default	admin	Telnet			
< No Access >					
wireless	admin	SSH	******	******	******

Displaying AuthCredentials 1 - 3 of 3

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

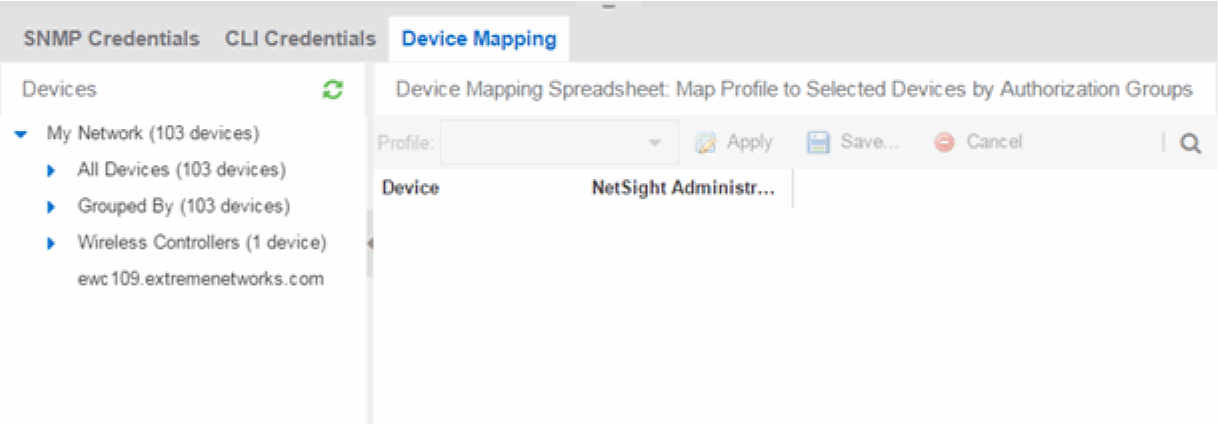
Opens the Add/Edit CLI Credential window where you can modify a CLI credential selected from the CLI Credentials table.

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.


SNMP Credentials
CLI Credentials
Device Mapping
Devices
My Network (103 devices)
All Devices (103 devices)
Grouped By (103 devices)
Wireless Controllers (1 device)
ewc109.extremenetworks.com
Device Mapping Spreadsheet: Map Profile to Selected Devices by Authorization Groups
Profile:
Apply
Save...
Cancel
Device
NetSight Administr...

Device Tree

The left panel contains a device tree, where you select a device or device group to view or configure.

Profile/Device Mapping Table

This table lists all of the selected devices and shows a column for the **NetSight (Extreme Management Center) Administrator Group** and each *Authorization Group* you defined. The *NetSight Administrator* column shows the profile used by the Extreme Management Center Administrator group. The Profile listed/selected for each Authorization Group column used by that group when communicating with the associated device and, as a result, defines the level of access granted to users that are members of that Authorization Group.

Select a **Profile** from the drop-down menu, click the authorization groups to which you want to apply the profile, and click **Apply**.

Apply Button Apply

Sets the profile selected in the **Profile** drop-down menu as the profile for the Authorization Groups selected in the table.

Save Button Save...

Saves your changes on the device or devices selected.

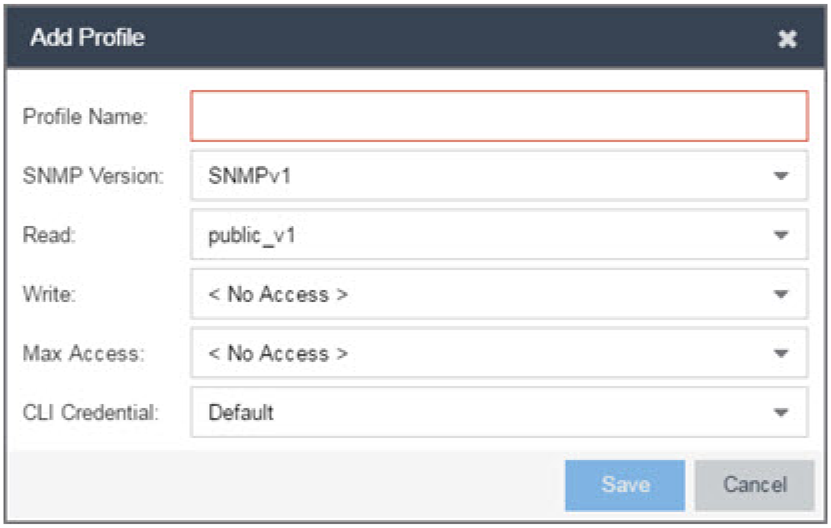
Cancel Button Cancel

Discards your unsaved changes.

Add/Edit Profile Window

This window lets you select the SNMP and CLI Credentials for a new profile or modify the credentials for an existing profile.

NOTE: When configuring profiles for ExtremeWireless Controllers, ensure the controllers are discovered using an SNMPv2c or SNMPv3 profile. This profile must also contain SSH CLI credentials for the controller. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers.



Profile Name:

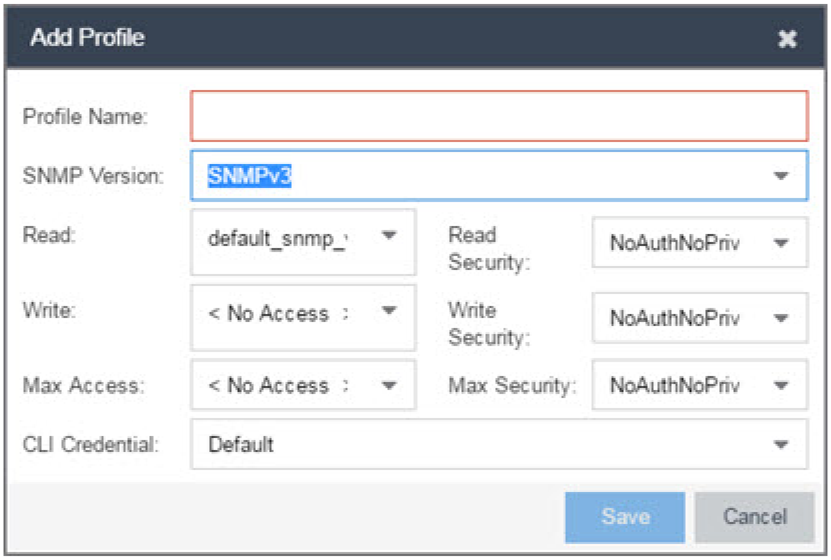
SNMP Version: SNMPv1

Read: public_v1

Write: < No Access >

Max Access: < No Access >

CLI Credential: Default



Profile Name:

SNMP Version: SNMPv3

Read: default_snmp_

Read Security: NoAuthNoPriv

Write: < No Access >

Write Security: NoAuthNoPriv

Max Access: < No Access >

Max Security: NoAuthNoPriv

CLI Credential: Default

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:

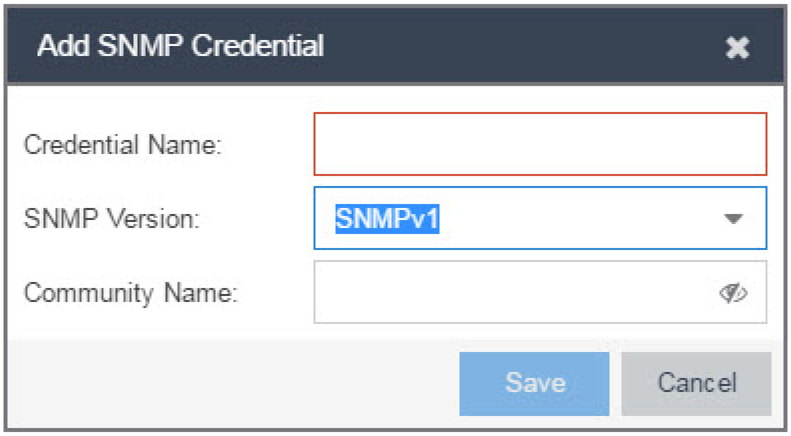
- AuthPriv — Highest security level requiring authentication and privacy (encrypted information).
- AuthNoPriv — Requires authentication, but unencrypted information.
- NoAuthNoPriv — Neither authentication nor privacy required.

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

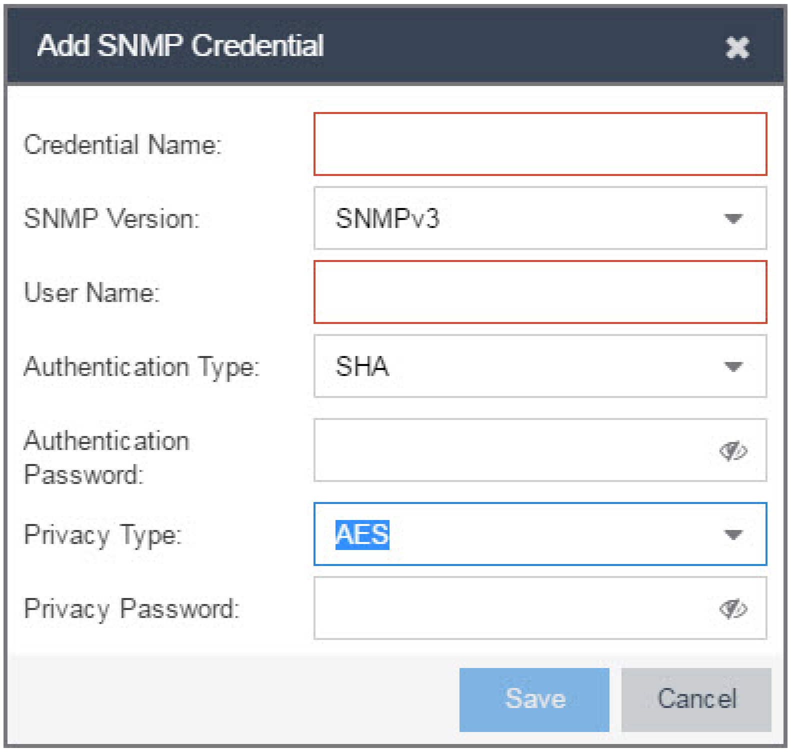
This window lets you define or edit the names and community names/passwords for SNMP credentials.


Add SNMP Credential

Credential Name:

SNMP Version: SNMPv1

Community Name:


Add SNMP Credential

Credential Name:

SNMP Version: SNMPv3

User Name:

Authentication Type: SHA

Authentication Password:

Privacy Type: AES

Privacy Password:

Credential Name

A unique name (up to 32 characters) assigned to this access credential. You can define a new credential or select a name from the table to modify settings for an existing credential. You cannot edit the name of an existing credential.

SNMP Version

This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2, or as SNMPv3. When either SNMPv1 or SNMPv2 is selected, the window provides fields where you can configure access levels using Community

Names. With SNMPv3 selected, you can configure access levels using Authentication and Privacy Types.

Community Name

For SNMPv1 or SNMPv2 credentials, this is the Community Name used for device access.

User Name

For SNMPv3 credentials, this is the User Name used for device access.

Authentication Type

For SNMPv3 credentials, select MD5, SHA1, or None, from this drop-down menu.

Authentication Password

This is the password (between 1 and 64 characters in length) used to determine Authentication. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Privacy Type

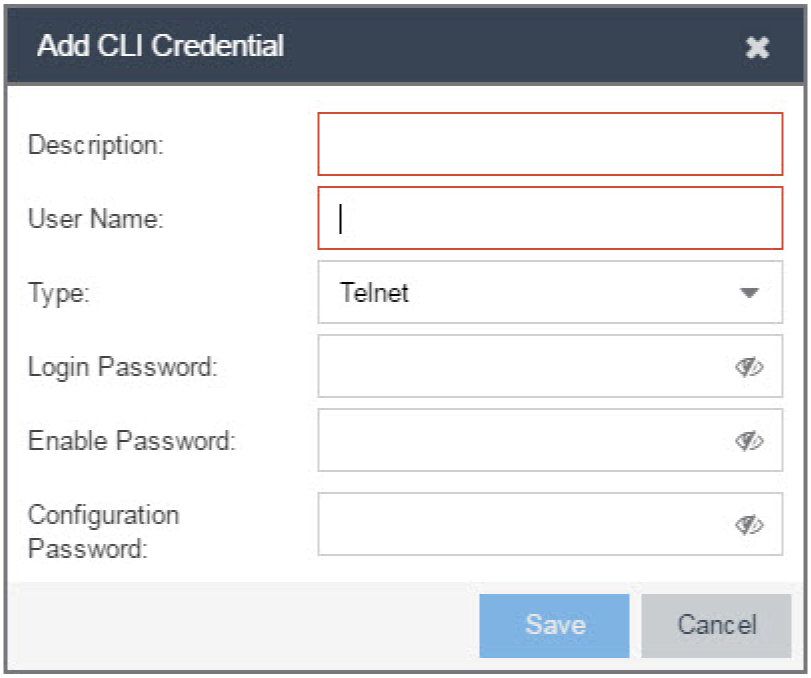
For SNMPv3 credentials, select DES or None from this drop-down menu.

Privacy Password

This is the password (between 1 and 64 characters in length) used to determine Privacy. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Add/Edit CLI Credential Window

This window lets you define or edit the user name and passwords for a CLI credential.



Description

A description of the credential.

User Name

The User name used for device access.

Type

The communication protocol used for the connection (SSH or Telnet).

Passwords

The passwords used to determine different levels of access to the device:

- Login — The password required to start a CLI session. Select the **Eye** icon to display your password.
- Enable — The password for entering Enable mode. Select the **Eye** icon to display your password.
- Configuration — The password for entering Configure mode. Select the **Eye** icon to display your password.

NOTE: When configuring CLI Credentials for ExtremeWireless Controllers, you must add the username and password Login credentials for the controller to this Add/Edit Credential window in order for Wireless Manager to properly connect (SSH) to the controller and read device configuration data. However, the Login password must be added to the Configuration password field instead of the Login password field. The username and Configuration password specified here must match the username and Login password configured on the controller.

Related Information

For information on related windows:

- Users/Groups Tab
- Site Tab

Vendor Profiles

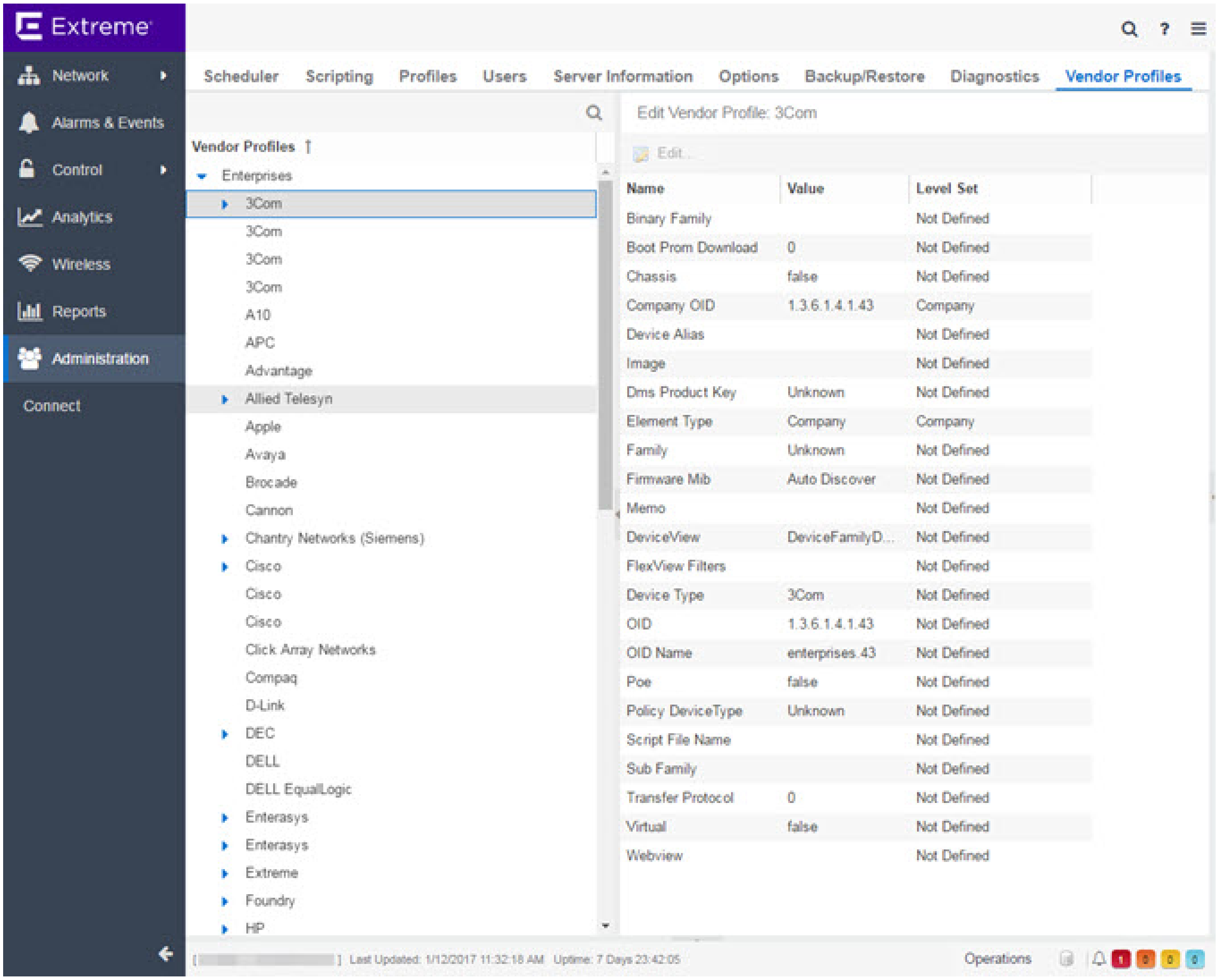
The **Vendor Profiles** tab allows you to add new device families to Extreme Management Center, which determines the reports available for the device in its DeviceView, the FlexView filters available for the device, and the scripts that apply to the device.

Vendor Profiles are a beta feature and are only available by selecting **Enable Beta Features** on the **Administration** > Diagnostics tab.

IMPORTANT: Only make changes to this tab if you are an expert user. Incorrectly configuring this tab causes significant adverse effects in Extreme Management Center and may require you to reinstall.

The **Vendor Profiles** tab is organized into two panels, the left panel contains a list of companies that manufacture networking devices. Nested within the company folder, if a device is part of a series of devices (known in Extreme Management Center as a device family), are folders for each device family. Within the device family folder are the individual device types that are a part of that device family. Any changes made at the company or device family level also apply to the devices within that folder, however you can overwrite the default configurations by changing a device family or individual device.

The right panel contains the vendor profile for the company, device family, or device you select in the left panel.



Vendor Profiles

- Enterprises
  - 3Com
  - 3Com
  - 3Com
  - 3Com
  - A10
  - APC
  - Advantage
  - Allied Telesyn
  - Apple
  - Avaya
  - Brocade
  - Cannon
  - Chantry Networks (Siemens)
  - Cisco
  - Cisco
  - Cisco
  - Click Array Networks
  - Compaq
  - D-Link
  - DEC
  - DELL
  - DELL EqualLogic
  - Enterasys
  - Enterasys
  - Extreme
  - Foundry
  - HP

Edit Vendor Profile: 3Com

Name	Value	Level Set
Binary Family		Not Defined
Boot Prom Download	0	Not Defined
Chassis	false	Not Defined
Company OID	1.3.6.1.4.1.43	Company
Device Alias		Not Defined
Image		Not Defined
Dms Product Key	Unknown	Not Defined
Element Type	Company	Company
Family	Unknown	Not Defined
Firmware Mib	Auto Discover	Not Defined
Memo		Not Defined
DeviceView	DeviceFamilyD...	Not Defined
FlexView Filters		Not Defined
Device Type	3Com	Not Defined
OID	1.3.6.1.4.1.43	Not Defined
OID Name	enterprises.43	Not Defined
Poe	false	Not Defined
Policy DeviceType	Unknown	Not Defined
Script File Name		Not Defined
Sub Family		Not Defined
Transfer Protocol	0	Not Defined
Virtual	false	Not Defined
Webview		Not Defined

Last Updated: 1/12/2017 11:32:18 AM Uptime: 7 Days 23:42:05

Vendor Profiles List

The left-panel of the **Vendor Profiles** tab contains a list of device vendors, displayed in alphabetical order. For those vendors with multiple products listed in Extreme Management Center, click the arrow icon beside the vendor name to display additional options related to that vendor. If the vendor's products are organized into product "families", or groups of products of the same type, the product family displays when expanding a vendor. Expanding the product family or a vendor with no product family displays individual devices for that vendor.

Select a vendor, product family, or product to open the vendor profile details in the right-panel.

Vendor Profile Details

The right-panel of the **Vendor Profiles** tab displays details related to the vendor, device family, or device selected in the left-panel Vendor Profiles list. The configuration of these fields determines how Extreme Management Center displays the element selected in the left-panel. Additionally, Extreme Management Center uses this information to determine the reports, filters, and scripts that apply to a device.

Related Information

For information on related windows:

- Users/Groups Tab
- Site Tab

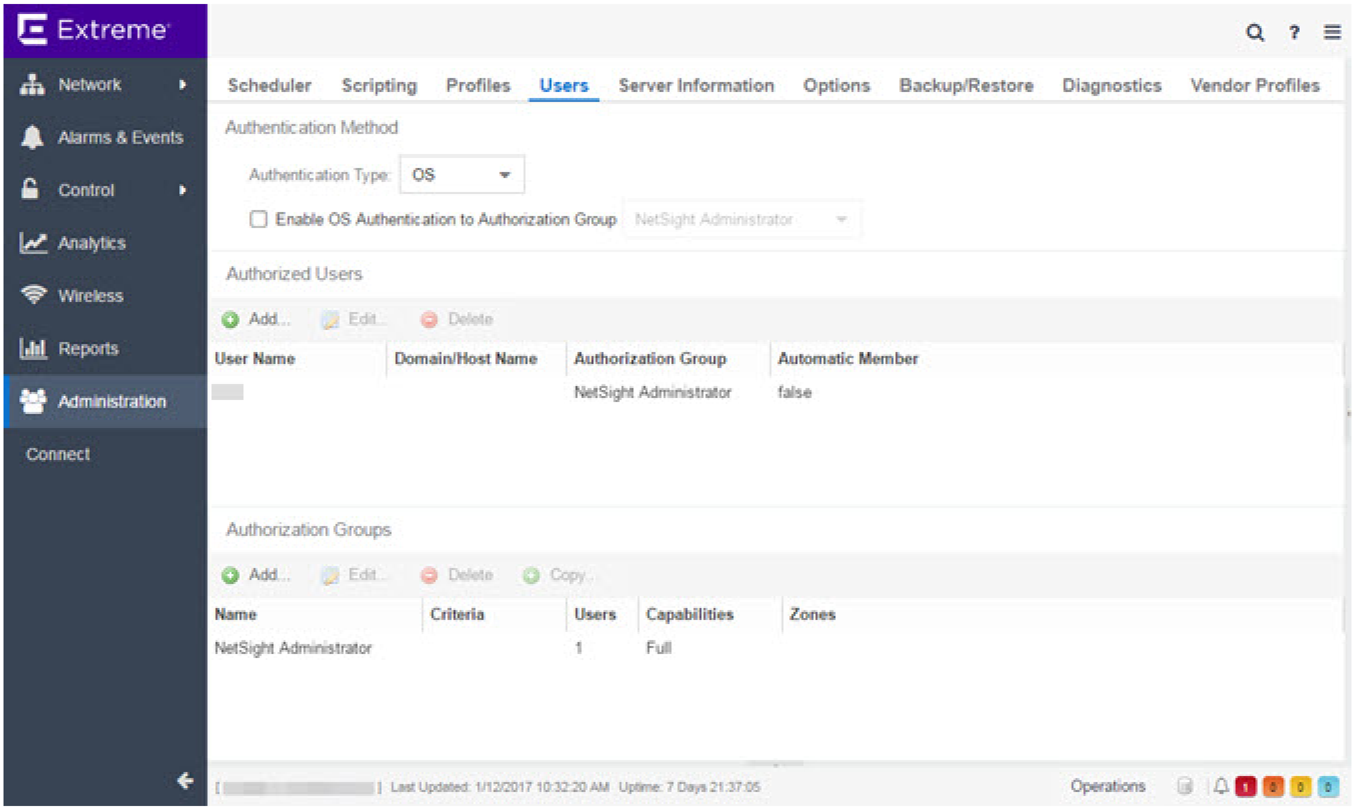
Users

Use the **Users** tab to create the authorization groups that define the access privileges (called *Capabilities*) to specific Extreme Management Center application features. When a user successfully authenticates, they are assigned membership in an authorization group. Based on their membership in a particular group, users are granted specific capabilities in the application. For example, create an authorization group called "IT Staff" that grants access to a wide range of capabilities and another authorization group called "Guest" grants a very limited range of capabilities.

The tab is also where you define the method used to authenticate users using Extreme Management Center. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

NOTE: When changes to authentication and authorization configurations are made, clients must restart in order to be subject to the new configuration. Disconnect those clients affected by the changes made to your authentication and authorization configurations. Use the Client Connections tab in the Server Information window to help identify which clients are affected by the changes, and disconnect those clients.

For instructions about how to add authorized users in Extreme Management Center, see How to Add Users in Extreme Management Center.



Authentication Method

Authentication Type: OS

☐ Enable OS Authentication to Authorization Group: NetSight Administrator

Authorized Users

User Name	Domain/Host Name	Authorization Group	Automatic Member
[redacted]		NetSight Administrator	false

Authorization Groups

Name	Criteria	Users	Capabilities	Zones
NetSight Administrator		1	Full	

[[redacted]] Last Updated: 1/12/2017 10:32:20 AM Uptime: 7 Days 21:37:05

Users/Groups Access

Click the **Acquire Lock** button to make changes to the **Users** tab. Only one user can make changes to the fields on this tab at one time, so clicking this button restricts access to other users.

Once you are finished making changes, click the button again to release the lock.

Authentication Method

Use this section to configure the method used to authenticate users who are attempting to launch a Extreme Management Center client or access the Extreme Management Center database using the Extreme Management Center Server Administration web page.

The following authentication methods are available:

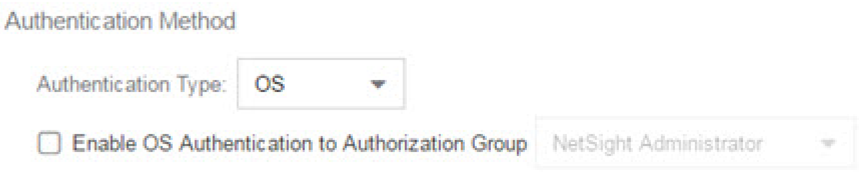
- OS Authentication *(the default)*
- LDAP Authentication

- RADIUS Authentication

WARNING: Changes to the **Authentication Type** are automatically saved to the server, which can prevent access to users.

OS Authentication (Default)

With this authentication method, the Extreme Management Center Server uses the underlying host operating system to authenticate users. Use the Authorized Users table to create a list of users allowed access and define their access capabilities.



Authentication Method

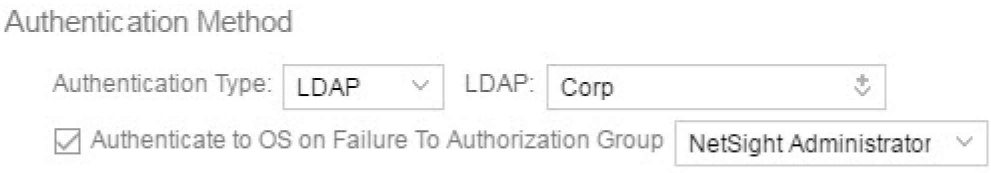
Authentication Type: OS

☐ Enable OS Authentication to Authorization Group NetSight Administrator

If desired, enable Automatic Membership and specify an authorization group. The Automatic Membership feature allows the operating system to authenticate a user who is not manually added to the Authorized Users table, dynamically add that user to the table, and assign that user to the specified authorization group the first time they log in. These users are indicated by a **true** in the Automatic Member column of the Authorized Users table.

LDAP Authentication

With this authentication method, the Extreme Management Center Server uses the specified LDAP configuration to authenticate users.



Authentication Method

Authentication Type: LDAP LDAP: Corp

☑ Authenticate to OS on Failure To Authorization Group NetSight Administrator

Use the drop-down menu to select the LDAP configuration for the LDAP server on your network that you want to use to authenticate users. Use the **New** menu option to add a new configuration or select the **Manage** option to manage your LDAP configurations.

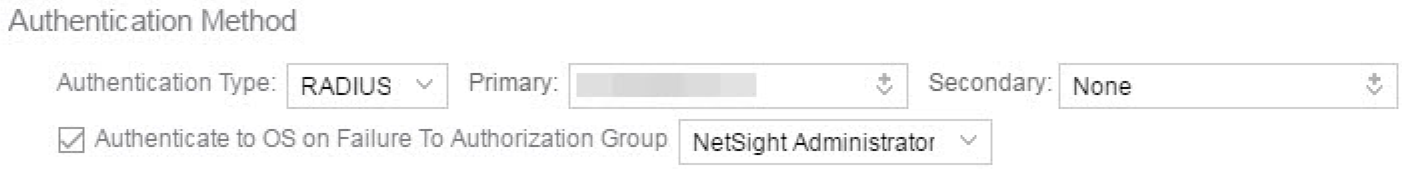
With LDAP Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, create an authorization group that matches everyone in a particular organization, department, or location. When a user authenticates, the attributes associated with that user are matched against a list of criteria specified as part of each authorization group. The first group with criteria met by the user's attributes becomes the authorization group for that user. The user is then added to the Authorized Users table as an automatic member, with that authorization group.

The **Authenticate to OS on Failure To Authorization Group** feature provides the option to use OS Authentication automatic membership if the LDAP authentication fails. Users authenticated by the operating system are dynamically assigned to the specified authorization group when they log in, and are automatically added to the Authorized Users table. These users are indicated by a **true** in the Automatic Member column of the table.

RADIUS Authentication

With this authentication method, the Extreme Management Center Server uses the specified RADIUS servers to authenticate users.

NOTE: The RADIUS Authentication mode supports the PAP authentication type.



Authentication Method

Authentication Type: RADIUS Primary: [redacted] Secondary: None

☑ Authenticate to OS on Failure To Authorization Group NetSight Administrator

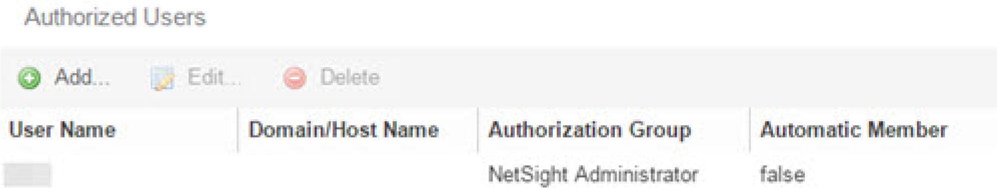
Use the drop-down menu to select the primary RADIUS server and backup RADIUS server (optional) on your network that you want to use to authenticate users. Use the **New** menu option to add a RADIUS server, or select **Manage** to manage your RADIUS servers.

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 Extreme Management Center database and allows you to add, edit, and delete users and define a user's membership in an authorization group. Each entry shows the user name and authorization group for the user and whether the user is an Automatic Member.



User Name	Domain/Host Name	Authorization Group	Automatic Member
[redacted]		NetSight Administrator	false

For users manually added to the Authorized Users table using this tab, the Automatic Member column is **false**. These users are granted permission to log in, no matter what the authentication setting is set to: OS Authentication, LDAP Authentication, or RADIUS authentication. All authentication methods allow the non-automatic users to log in.

User Name

The users added as authorized users.

Domain/Host Name

The user's domain/hostname used to authenticate to the Extreme Management Center database.

Authorization Group

The authorization group to which the user belongs.

Automatic Member

A value of **true** indicates that the user is automatically added to the authorization group via LDAP or RADIUS authentication, or the OS Authentication Automatic Membership feature. A value of **false** indicates that the user is an authorized user that was manually added to the table.

Add

Opens the Add/Edit User window, which allows you to define the username, domain, and authorization group for a new authorized user.

Edit

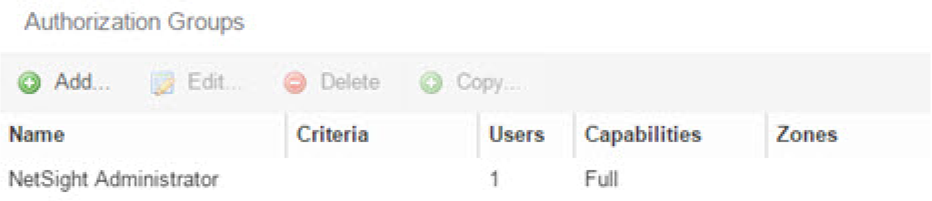
Opens the Add/Edit User window, which allows you to modify the authorization group membership for the selected user.

Delete

Removes the selected User from the Authorized Users table.

Authorization Groups Table

This table lists all of the authorization groups created. Authorization groups define the access privileges to the Extreme Management Center application features. Based on their membership in a particular authorization group, users are granted specific capabilities in the application.



Name	Criteria	Users	Capabilities	Zones
NetSight Administrator		1	Full	

When users are added to the Authorized Users table, they are assigned an authorization group. With LDAP or RADIUS authentication, users are dynamically assigned to authorization groups based on the attributes associated with that user in Active Directory. The attributes are used to match against a list of criteria specified as part of each authorization group. The groups are checked in the order they are displayed in this table, from top to bottom. The first group with criteria matched by the user's attributes becomes the effective authorization group for that user.

Every user must be assigned to a group. A user whose attributes don't match any of the criteria specified for any of the groups are not authenticated and are unable to log in. Create a "catch-all" group (for example, you could use objectClass=person for an LDAP Active Directory), whose criteria is very generic and whose capabilities are highly restricted to allow access to these unauthenticated users. This helps differentiate between a user who cannot authenticate successfully, and a user who does not belong to any group.

Name

This is the name assigned to the group. The Extreme Management Center Administrator group is created during installation and is granted Full capabilities and access. This group cannot be deleted or changed, but its capabilities can be viewed.

Precedence

This column, hidden by default, is available if the Authentication Method is LDAP or RADIUS. This indicates the order of precedence when a user is a member of multiple authorization groups. The authorization group with the higher precedence is the group to which the user is assigned. Use the Up Arrow and Down Arrow buttons to change the order of precedence for the authorization groups.

Criteria

This column displays the membership criteria defined for the associated group.

Users

This is the number of current members in the associated group.

Capabilities

This column summarizes the capabilities granted to the associated group: Full (all capabilities) or Customized (a subset of capabilities).

SNMP Redirect

This column, hidden by default, indicates whether users in the authorization group can edit the setting for Client/Server SNMP Redirect.

Auto Group

This column, hidden by default, indicates whether the group allows users to be automatically added via LDAP or RADIUS authentication, or the OS Authentication Automatic Membership feature.

Zones

This column displays the end-system zones to which users in the authorization group have access.

Add

Opens the Add/Edit Group window, which allows you to define the capabilities and settings for a new group.

Edit

Opens the Add/Edit Group window, which allows you to modify the capabilities and settings for a selected group.

Delete

Removes the selected group from the Groups table.

Copy

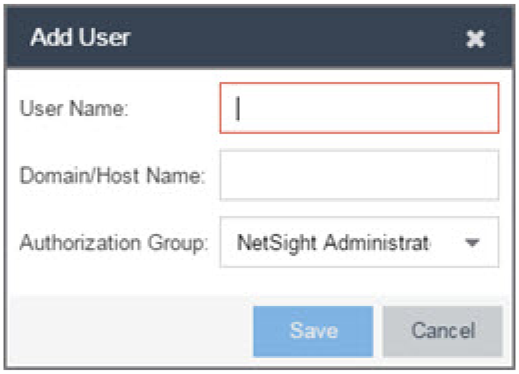
Duplicates the selected group from the Groups table and creates a new group with identical capabilities.

Up Arrow and Down Arrow

Changes the order of precedence for the authorization groups.

Add/Edit User Window

This window lets you define a user's user name, domain, and membership in an authorization group. This information is used to authenticate the user to the Extreme Management Center database.



Add User

User Name:

Domain/Host Name:

Authorization Group: NetSight Administrat

User Name

The name used for this authorized user.

Domain/Host Name

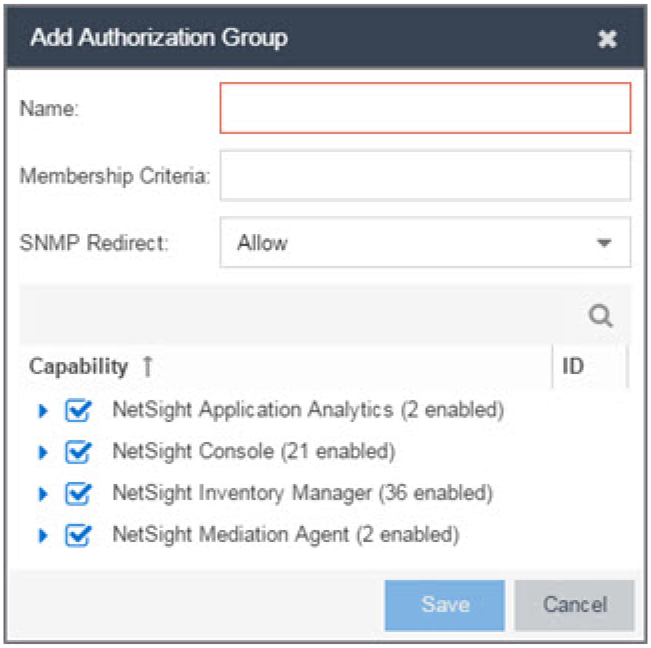
The user's domain/hostname used to authenticate to the Extreme Management Center database.

Authorization Group

Use the drop-down menu to select the authorization group to which the user is added.

Add/Edit Group Window

This window lets you define a new authorization group or edit an existing group. For additional information, see Authorization Group Capabilities.



Add Authorization Group

Name:

Membership Criteria:

SNMP Redirect: Allow

Capability	ID
☑ NetSight Application Analytics (2 enabled)	
☑ NetSight Console (21 enabled)	
☑ NetSight Inventory Manager (36 enabled)	
☑ NetSight Mediation Agent (2 enabled)	

Name

This is the name given to the group. When adding a group, enter any text string that is descriptive of the members of this group.

Membership Criteria

When a user is successfully authenticated using LDAP or RADIUS authentication, the Active Directory attributes associated with that user are used to match against this list of criteria to determine membership in the authorization group. The criteria is entered as name=value pairs, for example, department=IT (LDAP) or Service-Type=Framed-User (RADIUS). A user must have the specified attribute with a value that matches the specified value in order to meet the criteria to belong to this group. Multiple name=value pairs may be listed using a semicolon (";") to separate them. However, a user is considered a member of the group if they match at least one of the specified criteria; they do not need to match all of them.

NOTE: Extreme Management Center Administrator Group does not allow you to define membership criteria. Membership in the administrator group must be assigned manually using the Authorized Users table.

SNMP Redirect

- ALLOW — Lets users edit the setting for Client/Server SNMP Redirect.
- ALWAYS — Redirects all SNMP requests to the Extreme Management Center Server, regardless of the setting for Client/Server SNMP Redirect.
- NEVER — Never redirects SNMP requests to the Extreme Management Center Server, regardless of the setting for Client/Server SNMP Redirect.

Capability Tab

Expand the Capability tree in this tab and select the specific capabilities granted to users who are members of this group. The capabilities are divided into suite-wide and application-specific capabilities. Access to a particular capability is granted when it is checked in the tree. For a description of each capability, see Authorization Group Capabilities.

Related Information

For information on related windows:

- Profiles/Credentials Tab
- Site Tab

How to Add Users

Users are given access to parts of Extreme Management Center based on the authorization group to which they are assigned. Assign a set of capabilities for each authorization group and then add users to each authorization group depending on the capabilities they require.

NOTE: This topic assumes devices are already added to the Extreme Management Center database. For additional information on discovering and adding devices, see How to Discover Devices in Extreme Management Center.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

When you first log into Extreme Management Center the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to Extreme Management Center, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: Extreme Management Center does not save passwords. Users you create are authenticated against the Operating System, the RADIUS server, or the LDAP server, depending on the authentication method you select.

Create Authorization Groups

First, create authorization groups for each group of Extreme Management Center users.

1. Access the **Administration** > Users tab.
2. Click the **Acquire Lock** button in the Users/Groups Access section at the top of the tab.
   This button locks access to the tab for all other users and allows you to make changes to the authorization groups and authorized users.

3. Click the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using Extreme Management Center.
   The Capability section of the window allows you to expand each capability tree by selecting the arrow to the left of the checkbox to display more specific tasks. Select only those that apply to each user group. Additionally, you can search for a specific capability in the **Search** field above the tree.
5. Click the **Save** button to create the authorization group.
6. Repeat the process to create the necessary authorization groups.

Add Users to Authorization Groups

Next, use of the **Administration** > **Users** tab to create the users who require access to Extreme Management Center and add them to an authorization group depending on the level of access they require.

1. Click the **Add** button in the Authorized Users section.
2. Enter a User Name, a Domain/Host Name (if necessary), and select the Authorization Group with the appropriate level of access for the user.
3. Click the **Save** button to save the new user.
4. Repeat the process to add all Extreme Management Center users for each authorization group.

Select the Authentication Method

Finally, use **Administration** > **Users** tab to select the method by which users authenticate when accessing Extreme Management Center.

Extreme Management Center supports three authentication methods to authenticate users: using the underlying host operating system, using a specified LDAP configuration, or using specified RADIUS servers.

1. Select the **Authentication Type** using the drop-down menu in the Authentication Method section.
   The options change based on the **Authentication Type** selected.
2. Select the supplemental information based on the type selected.
3. Click the **Release Lock** button to allow other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

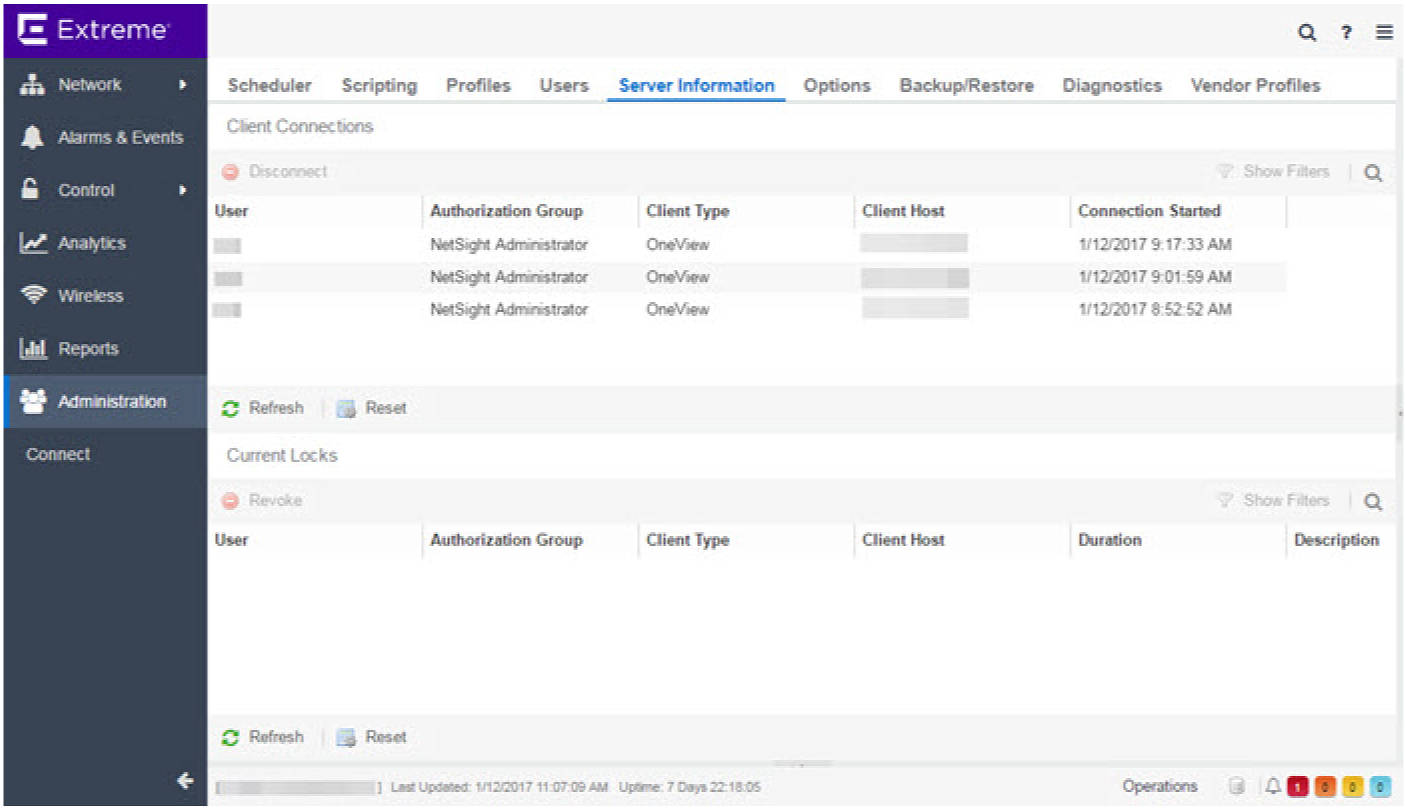
Related Information

For information on related topics:

- Users
- Authorization Group Capabilities

Server Information

The **Server Information** tab lets you view and manage Extreme Management Center client connections and locks. You must be assigned the appropriate user capabilities to access and use this tab.



User	Authorization Group	Client Type	Client Host	Connection Started
[redacted]	NetSight Administrator	OneView	[redacted]	1/12/2017 9:17:33 AM
[redacted]	NetSight Administrator	OneView	[redacted]	1/12/2017 9:01:59 AM
[redacted]	NetSight Administrator	OneView	[redacted]	1/12/2017 8:52:52 AM

User	Authorization Group	Client Type	Client Host	Duration	Description

[redacted] Last Updated: 1/12/2017 11:07:09 AM Uptime: 7 Days 22:18:05

Client Connections

The Client Connections table lists all of the currently connected clients for this server, with the most recent connection at the top. The list is automatically updated when clients connect or disconnect.

User

The name of the user that has connected to the server as a client.

Authorization Group

The authorization group to which the user belongs.

Client Type

The type of client, Console or another Extreme Management Center application.

Client Host

The name of the client host machine.

Connection Started

The date and time the client connection started.

Disconnect Button

This button disconnects the selected client. The client being disconnected receives a message saying that their connection will be terminated in 30 seconds. You must be assigned the appropriate user capability to disconnect clients.

Current Locks

The Current Locks table lets you view a list of currently held operational locks. Operational locks are used to control the concurrency of certain client/server operations. They are used in two ways:

- to lock a device while a critical operation is being performed, such as a firmware download.
- to lock a certain function so that only one user can access it at a time. For example, only one user can make changes to the **Users** tab at a time.

In the Current Locks table you can view information about each lock, such as who owns the lock, the duration of the lock, and a description of the lock. You can cancel a lock by selecting it in the table and clicking the **Revoke** button. When a lock is revoked, a message is displayed on the user's machine informing them that their use of the locked functionality is terminated. When the user acknowledges the message, the function closes. You must be assigned the appropriate user capability to revoke a lock.

User

The name of the user who initiated the lock.

Authorization Group

The authorization group the user belongs to.

Client Type

The type of client: Console or another Extreme Management Center application.

Client Host

The client host machine.

Duration

The amount of time the lock has been held.

Description

A description of the lock.

Refresh Button

This button refreshes the table and obtains updated lock information.

Revoke Button

This button removes the selected lock. When a lock is revoked, a message displays on the user's machine informing them their use of the locked functionality is terminated. When the user acknowledges the message, the function closes.

Related Information

For information on related tabs:

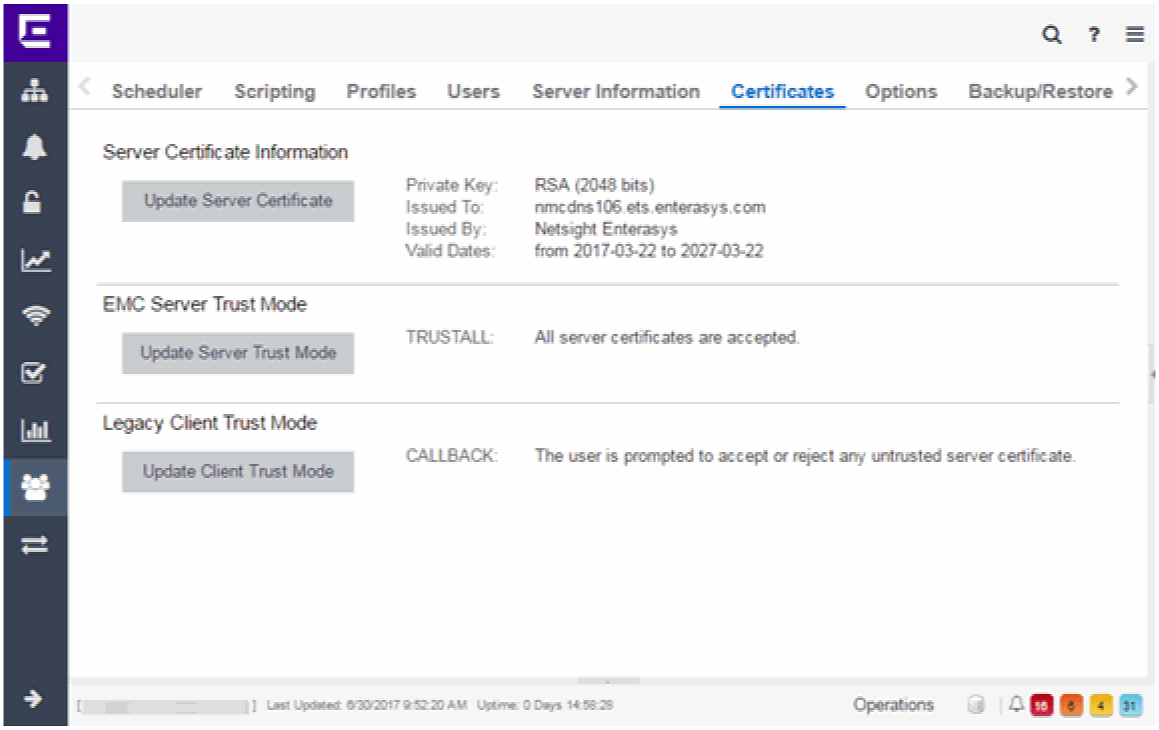
- Users

Extreme Management Center Certificates

The **Certificates** tab provides a central location for managing certificates in Extreme Management Center.

Use this tab to perform the following:

- Update the Extreme Management Center server certificate by replacing the server private key and certificate.
- View and change the server trust mode that specifies how servers in the Extreme Management Center deployment handle certificates from other servers.
- View and change the client trust mode that specifies how legacy java application clients handle a server certificate.



Server Certificate Information

Private Key: RSA (2048 bits)
Issued To: nmcdns106.ets.enterasys.com
Issued By: Netsight Enterasys
Valid Dates: from 2017-03-22 to 2027-03-22

EMC Server Trust Mode

TRUSTALL: All server certificates are accepted.

Legacy Client Trust Mode

CALLBACK: The user is prompted to accept or reject any untrusted server certificate.

Last Updated: 6/30/2017 9:52:20 AM Uptime: 0 Days 14:58:28

Server Certificate Information

Click the **Update Server Certificate** button to open the Update Server Certificate window, where you can replace the Extreme Management Center server private key and certificate. For information and steps on how to update the certificate, see How to Update the Server Certificate.

XMC Server Trust Mode

This section displays the current server trust mode that specifies how servers in the Extreme Management Center deployment handle certificates from other servers. Click the **Update Server Trust Mode** button to open the Update Server Certificate Trust Mode window, where you can change the server trust mode.

Legacy Client Trust Mode

This section displays the current client trust mode that specifies how legacy java application clients handle a server certificate. Click the **Update Client Trust Mode** button to open the Update Client Certificate Trust Mode window, where you can change the client trust mode.

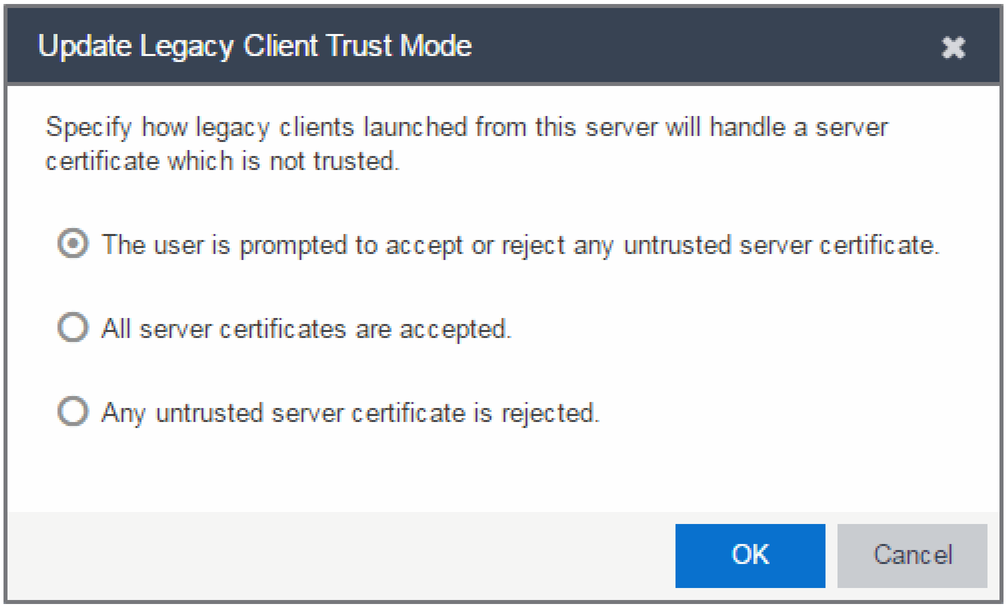
Related Information

For information on related windows:

- Update Server Certificate Window
- Update Server Certificate Trust Mode Window
- Update Client Certificate Trust Mode Window

Extreme Management Center Update Legacy Client Trust Mode Window

This window lets you update the client certificate trust mode that specifies how Extreme Management Center legacy java application clients handle the server certificates they receive. This option is only applicable if you use legacy java applications. Access this window from the Administration > Certificates tab.



Update Legacy Client Trust Mode

Specify how legacy clients launched from this server will handle a server certificate which is not trusted.

● The user is prompted to accept or reject any untrusted server certificate.

○ All server certificates are accepted.

○ Any untrusted server certificate is rejected.

Extreme Management Center use server certificates to provide secure communication between the Extreme Management Center server and legacy java application clients. When a server certificate is replaced, Extreme Management Center clients must be configured to trust the new certificate. A trust mode is used to determine how all clients handle updated certificates. You can set the client trust mode to one of the following options:

The user is prompted to accept or reject any untrusted server certificate.

If a client encounters a new certificate that is does not trust, the user is prompted to either accept or reject the new certificate. If the server certificate is replaced and the user expects to see the new certificate, then they can accept the certificate if it is correct. If the server certificate is not replaced and the client inadvertently connected to a server that is not trusted, then the user can reject the certificate.

All server certificates are accepted.

All server certificates are accepted without a trust check. Use this option if there is no possibility for an untrusted client to connect to a server and the user does not need to be prompted to accept or reject a new certificate.

Any untrusted server certificate is rejected.

If a client encounters a new certificate that is does not trust, the certificate is rejected and the client connection fails. While this option is the most secure, if the server certificate is replaced, the new certificate is rejected. If you are replacing a server certificate, do not use this trust mode until all clients indicate they trust the new certificate.

For more information on how to use trust modes, see Advanced Security Options in the Secure Communication Help topic.

Related Information

For information on related windows:

- Certificates Tab
- Update Server Certificate Trust Mode Window

Extreme Management Center Update Server Certificate Window

The Extreme Management Center server uses a private key and server certificate to provide secure communication for administrative web pages, Extreme Management Center and Extreme Access Control Dashboard tools, and for internal communication between servers. The Update Server Certificate window lets you replace the Extreme Management Center server certificate. You can access this window from the Administration > Certificates tab.

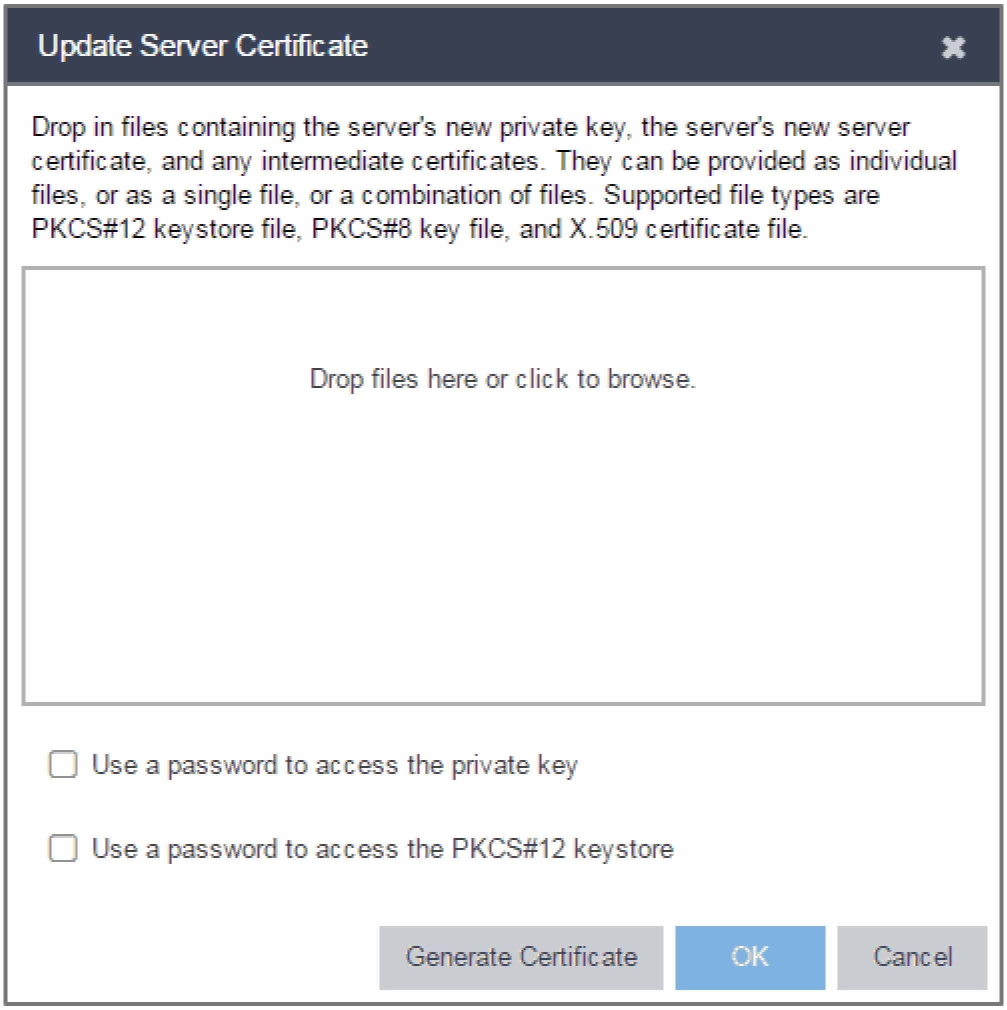
During installation, Extreme Management Center generates a unique private server key and server certificate. While these provide secure communication, there may be cases where you want to update the Extreme Management Center server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which Extreme Management Center must communicate. Additionally, you may want to use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages. For complete instructions on replacing and verifying the certificate, see How to Update the Server Certificate.

After you have updated the certificate, you must restart the Extreme Management Center server to deploy the new private key and server certificate.

NOTE: Whenever the Extreme Management Center server certificate is changed, other Extreme Management Center components may be affected by the change and stop trusting the server. You can specify how Extreme Management Center clients and other servers handle updated certificates by configuring the client trust mode and server trust mode settings. Before updating the Extreme Management Center server certificate, be sure that the client and server trust modes are configured to trust the new certificate. For more information, see Update Client Certificate Trust Mode window and Update Server Certificate Trust Mode window.

Drag and drop files containing the private key, the server certificate, and any intermediate (chained) certificates provided by the certificate authority. Add the files in any order. For complete instructions on replacing and verifying the certificate using this option, see How to Update the Extreme Management Center Server Certificate.

NOTE: Provide certificates for all certificate authorities that need to be trusted. You cannot append to an existing list.



Update Server Certificate

Drop in files containing the server's new private key, the server's new server certificate, and any intermediate certificates. They can be provided as individual files, or as a single file, or a combination of files. Supported file types are PKCS#12 keystore file, PKCS#8 key file, and X.509 certificate file.

Drop files here or click to browse.

☐ Use a password to access the private key

☐ Use a password to access the PKCS#12 keystore

Use a password to access the private key

Select the checkbox and supply the private key password in the field, if the private key is encrypted with a password. If you do not have the private key, refer to the instructions for generating them.

Use a password to access the PKCS#12 keystore

Select the checkbox and supply the keystore password in the field, if the PKCS#12 keystore is protected with a password.

Generate Certificate

Click **Generate Certificate** to automatically generate a new private key and certificate using the same method that occurs when Extreme Management Center is installed. Using this method does not require you to provide any files or passwords.

OK

Click **OK** to save your changes.

Cancel

Click **Cancel** to close the window and discard your changes.

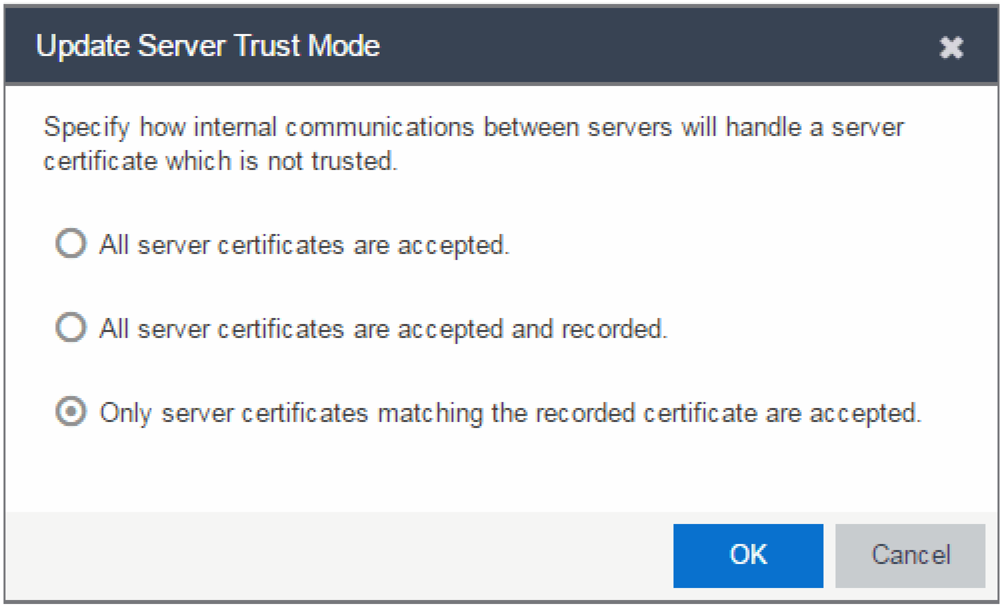
Related Information

For information on related topics:

- Certificates Tab
- Update Server Certificate Trust Mode Window
- Update Client Certificate Trust Mode Window

Extreme Management Center Update Server Trust Mode Window

This window lets you set the server certificate trust mode that specifies how all the servers in your Extreme Management Center deployment handles certificates received from other servers. Access this window from the Administration > Certificates tab.



Update Server Trust Mode

Specify how internal communications between servers will handle a server certificate which is not trusted.

○ All server certificates are accepted.

○ All server certificates are accepted and recorded.

● Only server certificates matching the recorded certificate are accepted.

Depending on your deployment, there can potentially many servers in Extreme Management Center and Extreme Access Control. For example, there is the Extreme Management Center server, the Extreme Access Control engine servers, and Extreme Access Control assessment servers. In addition, there may be external servers such as LDAP servers with which both Extreme Management Center and Extreme Access Control may communicate. As these different servers communicate, they use server certificates to determine whether or not they trust each other.

The trust mode is used to specify how the servers handle the certificates they receive from other servers. You can set the trust mode to one of the following options:

All server certificates are accepted.

All certificates from other servers are accepted without a trust check. This mode is primarily used while setting up a Extreme Management Center/Extreme Access Control deployment, and is also suitable when the network is sufficiently protected from spoofing attacks.

Use this mode when troubleshooting trust problems on the network. It allows the Extreme Management Center server to communicate with all Extreme Access Control engines, and configure those engines to accept all certificates. This restores any communication broken due to a trust issue and allows you to resolve the problem from Extreme Access Control.

All server certificates are accepted and recorded.

All certificates from other servers are accepted without a trust check. Additionally, each server records the certificate that it receives and associates that certificate with the sending server. In this way, each server builds their own set of recorded certificates, creating a list of certificates that they trust.

Use this mode initially until all servers build a complete set of required certificates and then change the mode to Only server certificates matching the recorded certificate are accepted. It is important to give this phase enough time so that connections between the various servers can take place and all certificates are recorded. Administrators must ensure that no servers are spoofed during the time this mode is used. When you are confident that all certificates are exchanged and recorded, change the trust mode to Only server certificates matching the recorded certificate are accepted.

Only server certificates matching the recorded certificate are accepted.

Any certificate from another server must match the certificate recorded for that server when the mode is set to All server certificates are accepted and recorded. If the server certificate does not match, then the server is not trusted.

This mode provides an extra level of security intended to detect and prevent someone from spoofing a server. If an IP address or hostname is hijacked and connections are routed to another server, that server is not trusted. While this mode is the most secure, if any server certificate is replaced, the new certificate is rejected. Therefore, if you are replacing a server certificate, select All server certificates are accepted and recorded until the new certificate is recorded.

When the trust mode is changed, the Extreme Management Center server is immediately changed to use the new mode. Extreme Access Control engines begin using the new trust mode when enforced.

For more information on how to use trust modes, see Advanced Security Options in the Secure Communication Help topic.

Related Information

For information on related topics:

- Certificates Tab
- Update Client Certificate Trust Mode Window

How to Update the Server Certificate

Extreme Management Center allows you to change the server key and certificate generated during installation. While these provide secure communication, you may want to update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which Extreme Management Center must communicate. You can also use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages.

You need a server private key and server certificate to perform the certificate replacement.

Some instructions in this Help topic use OpenSSL software to perform certain tasks. OpenSSL is available on the Extreme Management Center engine or can be downloaded from http://www.openssl.org. After downloading and installing OpenSSL, add the OpenSSL tool to your path using the instructions in How to Add OpenSSL to Your Path in the Secure Communication Help topic. Other software tools can be used to perform these tasks, if desired.

Instructions on:

- Certificate Requirements
- Replacing the Certificate
- Verifying the Certificate
- Generating a Server Private Key and Server Certificate

Certificate Requirements

Generate the server certificate using the RSA or DSA server private key (in PKCS #8 format). For "browser-friendly" certificates, the server certificate should identify the Extreme Management Center server by its fully qualified host name.

If your certificate authority (CA) provides additional intermediate certificates, provide those as well. Use the intermediate certificates in whatever format the CA provides them: in individual files, in a bundle file, or in the same file as the server certificate. Extreme Management Center also accepts PKCS#12 keystore files, which can contain both a private key and certificates. Enter the PKCCS#12 file here.

NOTE: Use the following OpenSSL command where <server.key> is the original non-PKCS #8 formatted key file to convert your key file to a PKCS #8 format. (OpenSSL is available on Extreme Management Center and Extreme Access Control engines. The server.key file can be copied and converted on either engine.)

```
     openssl pkcs8 -topk8 -in <server.key> -out server-pkcs8.key
-nocrypt
```

Replacing the Certificate

The following steps assume you generated a replacement server private key and server certificate.

NOTE: Whenever the Extreme Management Center server certificate is changed, other Extreme Management Center components may be affected by the change and stop trusting the server. Extreme Management Center clients and other servers must be configured to handle updated certificates using the client certificate trust mode and server certificate trust mode settings. Before updating the Extreme Management Center server certificate, be sure that the client and server trust modes are configured to trust the new certificate. For more information, see Update Client Certificate Trust Mode window and Update Server Certificate Trust Mode window.

To replace the server private key and server certificate:

1. Access the **Administration** > **Certificates** tab.
2. Click the **Update Server Certificate** button. The Update Server Certificate window opens.
3. Drag and drop a private key, certificate file, or a keystore file. Click in the box to browse for the file.

   A private key file must be encoded as a PKCS #8 file.

   Use a certificate file as the server certificate and any intermediate or chained certificates.

   Use a PKCS#12 keystore file to provide the private key, or certificates, or both.

4. Select **Use a password to access the private key** if the private key is encrypted in the key file or the keystore file. Enter the password in the field.
5. Select **Use a password to access the PKCS#12 keystore** if the keystore file is protected with a password. Enter the password in the field.
6. Click **OK**.

   A confirmation window listing your file information displays.
7. Confirm that the information you provided is correct.
8. Click **Yes** to proceed with the certificate replacement.

   The private key and server certificate updates on the Extreme Management Center server.
9. Restart the Extreme Management Center server to deploy the new private key and server certificate.

Verifying the Certificate

Once the new server certificate is installed and the server restarts, use one of the following methods to verify the server is now using the proper server certificate.

Use a Browser

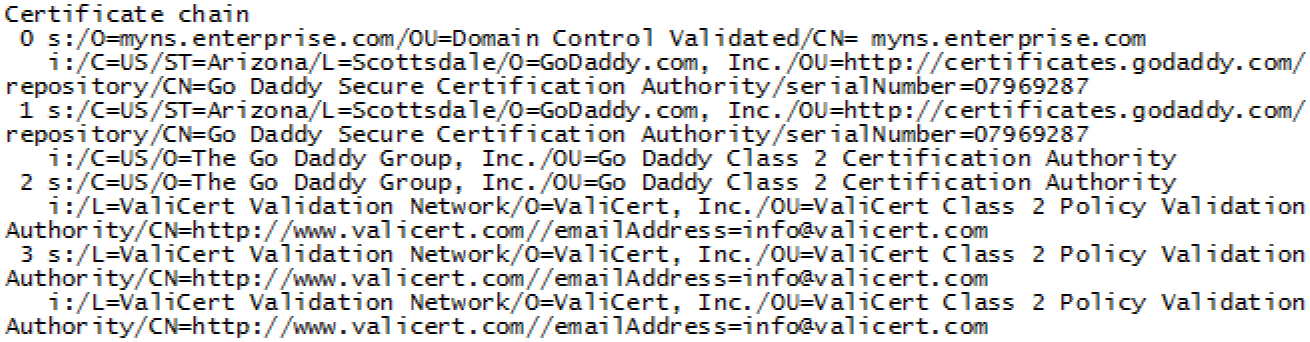
1. Access the Extreme Access Control Dashboard web page at `https://<NetSight Server FQDN>:8443/Monitor/jsp/nac/dashboard.jsp.` or the Extreme Management Center web page at `https://<NetSight Server FQDN>:8443/Monitor/jsp/reporting/reporting.jsp`.
2. Verify no browser warnings display when you access the web page, if using a "browser-friendly" certificate.
3. Use your browser to view the certificate used:
   - Internet Explorer 7.0 or later: View > Security Report > View Certificates
   - Mozilla Firefox 3.5 or later: Tools > Page Info > Security > View Certificates

Use OpenSSL

1. Use OpenSSL to test the server connection with the following command:

   ```
   openssl s_client -connect <NetSight Server IP>:8443
   ```

2. The output from this program includes a section titled "Certificate chain". This enumerates the certificates returned by the server. For each certificate, the Subject and the Issuer are displayed. With multiple certificates, if the certificates are in the proper order, the issuer of each certificate matches the subject of the following certificate. Here is a sample output from the program:

   ```
   Certificate chain
    0 s:/O=myns.enterprise.com/OU=Domain Control Validated/CN= myns.enterprise.com
      i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
   repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
    1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
   repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
      i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
    2 s:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
      i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
   Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
    3 s:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
   Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
      i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
   Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
   ```

3. Terminate the program by pressing [Ctrl]+C.

Generating a Server Private Key and Server Certificate

Generate a server private key and server certificate using the instructions in the sections below.

You need to:

1. Generate a server private key:

   a. Enter the following command to use OpenSSL to generate a password-encrypted PKCS #8 formatted server private key file. Use the key size and output file name you prefer. (If you are unsure of the key size, use 2048.)

      ```
            openssl genrsa <key size> | openssl pkcs8 -topk8
      -out <output file>
      ```

      For example:

      ```
      openssl genrsa 2048 | openssl pkcs8 -topk8 -out
      ```

```
server.key
```

   b. You are prompted for an Encryption Password. Be sure to make a note of the password that you enter. If the password is lost, you need to generate a new server private key and a new server certificate.

2. Create a Certificate Signing Request:

   a. Enter the following command to generate a CSR file. Use the output file name you used in step 1 above as the input file, and specify the output file name you prefer:

   ```
         openssl req -new -key <input file> -out <output file>
   ```

   For example:

   ```
         openssl req -new -key server.key -out server.csr
   ```

   b. You are prompted for information that appears in the certificate. When you are prompted for a Common Name, specify the fully qualified host name of the Extreme Management Center server. For example:

   ```
         Common Name (eg, YOUR name) []:netsight1.mycompany.com
   ```

3. Submit the request to a Certificate Authority or generate a self-signed certificate.

   The procedure for submitting a CSR to a Certificate Authority (CA) varies with the service used. Usually, it is done through a website using a commercial service such as VeriSign. You can also use an in-house CA, which generates certificates used internally by your enterprise. You provide information including the contents of the CSR, and receive back one or more files containing the server certificate and possibly other certificates to be used in a chain.

4. Verify the contents of the server certificate.

   It is important to verify that the new server certificate contains the data you supplied when creating the CSR. In particular, make sure the Common Name (CN) is the fully qualified host name of the Extreme Management Center server.

   Use OpenSSL to view the contents of the server certificate file server.crt using the following command:

   ```
         openssl x509 -in server.crt -text -noout
   ```

You can use the following steps regardless of whether you are using a commercial certificate authority or an in-house certificate authority.

Authorization Group Capabilities

As part of configuring Authorization and Device Access, users are assigned to authorization groups that define their access privileges to Extreme Management Center application features. These access privileges (called Capabilities) grant specific capabilities in the application. For example, you may have an authorization group called "IT Staff" that grants access to a wide range of capabilities, while another authorization group called "Guest" grants a very limited range of capabilities.

Capabilities are defined when you create an authorization group and assign users to the group by clicking the **Add** button in the Authorization Groups section of the **Administration** > **Users** tab. In the Add/Edit Authorization Group window, the Capability list displays all the various capabilities for your selection.

The capabilities are divided into suite-wide and application-specific capabilities. Checking a capability grants access to that capability.

The following sections provide a description of each capability:

- Extreme Management Center Application Analytics
- Extreme Management Center Console
  - Wireless Manager
  - VLAN Models
- Extreme Management Center Mediation Agent
- Extreme Management Center NAC Manager
- Extreme Management Center OneView
- Extreme Management CenterPolicy Manager
- Extreme Management Center Suite
  - Authorization/Device Access
  - Common Web Services
  - Credentials Web Service
  - Device Local Management WebView
  - Devices

  - Events and Alarms
  - Extreme Management Center All User Options
  - Server Information
  - ZTP+ Registration
- Northbound API
- Vendor Profiles
- Workflows

Extreme Management Center Application Analytics

Application Analytics Read Access

Allows the ability to access the **Analytics** tab and view the Application Analytics reports. The Application Analytics feature is available with the Extreme Management Center (NetSight) Advanced (NMS-ADV) license.

Application Analytics Read/Write Access

Adds the ability to view the **Analytics** > **Configuration** tab and configure Application Analytics engines and NetFlow and Application Telemetry Collecting devices. Also adds the ability to create and modify fingerprints.

Extreme Management Center Console

Launch a NetSight (Extreme Management Center) Console Client

Allows the ability to launch the Console application. An error message appears for users who do not have this capability when they attempt to launch Console.

MIB Tools

Allows the ability to launch MIB Tools from the Console menus.

Allow SNMP sets to Devices

Allows the ability to write SNMP sets to network devices.

Modify Compass SNMP MIBs

Allows the ability to select Compass SNMP MIBs in the Compass options panel.

Modify Device Access

Allows the ability to modify device access information in the Access Properties tab.

Show Passwords in Clear Text

Allows the ability to view passwords in clear text in various Console windows.

Device Manager

Allows the ability to launch Device Manager from a device.

TFTP Download

Allows the ability to perform a configuration upload/download or firmware image download on a device.

Trap Configuration

Allows the ability to launch and use the Trap Receiver Configuration window.

Configure FlexViews

Allows the ability to create and modify FlexViews.

Syslog Configuration

Allows the ability to launch and use the Syslog Receiver Configuration window.

Wireless Manager

Launch

Allows the ability to launch Wireless Manager from the Console Tools menu.

Configure

Allows the ability to configure Wireless Manager.

VLAN Models

View

Allows the ability to view VLAN Models using the VLAN Elements Editor, accessed from the **VLAN** tab in Console.

Configure

Allows the ability to configure VLAN Models using the VLAN Elements Editor, accessed from the **VLAN** tab in Console.

Extreme Management Center Mediation Agent

Read access to the Mediation Agent Web Services API

Provides the Application Analytics engine with read access to Extreme Management Center (Extreme Management Center) via web services API.

Read/Write access to the Mediation Agent Web Services API

Provides the Application Analytics engine with read/write access to Extreme Management Center via web services API.

Extreme Management CenterNAC Manager

Launch NAC Manager

Allows the ability to launch the NAC Manager application. Users who do not have this capability see an error message when they attempt to launch NAC Manager.

Edit NAC Manager Configuration

Allows the ability to edit all aspects of the NAC Manager configuration including rule components, NAC profiles, assessment, registration, and managing advanced configurations.

Force reauthentication and scan (assess) End-Systems

Allows the ability to force end-systems to be reauthenticated and scanned, but does not allow the ability to edit the NAC Manager configuration.

Read access to the NAC Web Services API

Provides read access to the NAC web service, which is a third-party integration point. The NAC web service exposes methods for manipulating NAC infrastructure components.

Read/write access to the NAC Web Services API

Provides read/write access to the NAC web service, which is a third-party integration point. The NAC web service exposes methods for manipulating NAC infrastructure components.

Read access to the NAC System Web Services APIs

Provides read access to the NAC System web services, allowing programmatic access to advanced web services that are not publicly documented.

Read/write access to the NAC System Web Services APIs

Provides read/write access to the NAC System web services, allowing programmatic access to advanced web services that are not publicly documented. Also provides the ability to use the NAC Request Tool.

Extreme Management Center OneView

Access OneView

Allows the ability to launch the Extreme Management Center web-application formerly known as OneView, but does not provide any Extreme Management Center report access. Selecting only this capability without any other capabilities would be the same as not allowing access to Extreme Management Center.

Access OneView Reports

Adds the ability to view all reports accessed from the **Reports** tab.

Access OneView Search

Adds the ability to use the **Search** tab.

Access OneView Administration

Adds the ability to access administration tools and enable data collection.

NetFlow Read Access

Adds the ability to view the **Flows** tab.

Maps

Allows the ability to perform the following map functions:

- Maps Read Access - Adds the ability to access the **Map** tab and view the maps.
- Maps Read/Write Access - Adds the ability to access the **Map** tab, and view and modify maps. This includes adding devices to the maps, drawing on the maps, changing map scale, and changing map properties (for example, the map name and background image).

Events and Alarms

Allows the ability to perform the following event and alarm functions:

- OneView Event Log Access - Allows the ability to view device information and event log details.
- OneView Alarms Read Access - Allows the ability to view current alarms in the **Alarms and Events** tab.
- OneView Alarms Read/Write Access - Allows the ability to view and clear alarms in the **Alarms and Events** tab.

FlexView

Allows the ability to perform the following OneView FlexView functions:

- OneView FlexView Read Access - Allows the ability to launch a FlexView from the **Network** tab.
- OneView FlexView Read/Write Access - Allows the ability to launch and edit a FlexView from the **Network** tab.

Identity and Access

Allows the ability to perform the following Extreme Access Control functions:

- Access OneView Control Reports - Provides access to the Dashboard view, System view, Health view, and Data Center view from the **Control** tab.
- OneView End-Systems Read Access - Provides access to the End-Systems view from the **Control** tab.
- OneView End-Systems Read/Write Access - Provides access to the End-Systems view from the **Control** tab, and allows the ability to perform actions such as forcing reauthentication and changing an end-system's group membership.
- OneView Group Read Access - Allows the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and view group information.
- OneView Group Read/Write Access - Allows the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and edit group information.

NetSight (Extreme Management Center) Manager Access

Adds the ability to access the NetSight (Extreme Management Center) Manager.

Extreme Management Center Policy Manager

Launch NetSight (Extreme Management Center) Policy Manager

Allows the ability to launch the Policy Manager application. Users who do not have this capability see an error message when they attempt to launch Policy Manager.

Read/Write capabilities for Policy Enforcement and Management

Allows the ability to manage and enforce policy to network devices using Policy Manager.

Read/Write access to the Policy Web Service APIs

Provides read/write access to the Policy web service, which is a third-party integration point. The Policy web service allows programmatic access to policy management.

Extreme Management Center Suite

The following capabilities apply to all Extreme Management Center applications.

Authorization/Device Access

View Authorization/Device Access

Allows the ability to view, but not to configure the Authorization/Device Access tool, accessed from the Tools menu in any Extreme Management Center application. Users who attempt to access the tool without this capability see an error message.

Configure Users, User Groups, and Capabilities

Allows access to the Users/Groups tab in the Authorization/Device Access tool and the ability to create and edit users and authorization groups.

Configure Profiles/Credentials

Allows access to the Profiles/Credentials tab in the Authorization/Device Access tool and the ability to define the SNMP credentials used to access network devices and the profiles that use those credentials.

Configure Profile/Device Mapping

Allows access to the Profile/Device Mapping tab in the Authorization/Device Access tool and the ability to specify the SNMP profiles each authorization group uses when communicating with each device.

Configure LDAP and RADIUS Servers

Allows the ability to configure RADIUS Servers and LDAP Configurations in the Users/Groups tab in the Authorization/Device Access tool.

Manage SNMP Passwords

Allows access to the Manage SNMP Passwords tab in the Authorization/Device Access tool and the ability to manage the credentials set on network devices.

Allow Tools to Use All Profiles

In MIB Tools, this capability allows users to select from all available profiles when using a Console profile to contact the device.

Allow View of No Access Devices

If an authorization group is configured with "No Access" to specific devices (in the Profile/Device Mapping tab), this capability allows members of that group to view the No Access devices in the left-panel tree, even though they cannot access the devices.

Common Web Services

Read access to the Web Services APIs2

Provides read access to the Extreme Management Center Common web service, which is a third-party integration point. The Common web service exposes methods for manipulating Extreme Management Center infrastructure components.

Read/write access to the Web Services APIs

Provides read/write access to the Extreme Management Center Common web service, which is a third-party integration point. The Common web service exposes methods for manipulating Extreme Management Center infrastructure components.

Credentials Web Service

Read operations

Provides read access to the Extreme Management Center Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

Read/write operations

Provides read/write access to the Extreme Management Center Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

Device Local Management WebView

Auto Login to Web Local Management for NAC Appliances

Allows the ability to launch local management for Extreme Access Controlengines without requiring a login for users with the necessary credentials. Users who do not have this capability are required to log in.

Auto Login to Web Local Management for ExtremeWireless Controllers

Allows the ability to launch local management for wireless controllers without requiring a login for users with the necessary credentials. Users who do not have this capability are required to log in.

Devices

Add, Discover, and Import

Allows the ability to add devices using the Add Device window, discover devices using the Discover tool, and import devices using the File > Device List > Import Devices option.

Configure Groups

Allows the ability to create device groups and add and remove devices to and from device groups.

Delete

Allows the ability to delete devices from the Extreme Management Center database.

Export

Allows the ability to export a device list using the File > Device List > Export option.

Configure Status Polling Options

Allows the ability to set suite-wide Status Polling options available from the Tools > Options window.

Execute Command Scripts

Allows the ability to execute command scripts (using the Command Script tool) on a device in Console or Inventory Manager.

Events and Alarms

Events

Allows the following Event configuration capabilities:

- View Event Logs - View event logs in all Extreme Management Center applications.
- View Events for No Access Devices - If you configured an authorization group with "No Access" to specific devices (in the Profile/Device Mapping tab), this capability allows members of that group to view events for the No Access devices, even though they cannot access the devices.
- Configure Event Options - Set suite-wide Event Logs options available from the Tools > Options window.
- Acknowledge Events - Acknowledge events in the event log.

- Configure Server Log Managers - Add, edit, and remove Log Managers using the Event View Manager window.
- Clear and Roll Server Log Managers - Clear and roll event logs on the Extreme Management Center Server using the button in the lower-right corner of the event log.

Alarms

Allows the following Alarm configuration capabilities:

- View - View alarms in the Event Log.
- Configure - Configure alarms using the Alarms Manager window.

Extreme Management Center (formerly NetSight) All User Options

These capabilities provide the ability to set suite-wide options that apply to all users, using the Tools > Options window.

Configure Services for NetSight (Extreme Management Center) Server Options

Allows the ability to specify TFTP settings.

Configure SMTP E-mail Options

Allows the ability to specify the SMTP E-Mail server used by the Extreme Management Center E-Mail notification feature.

Request and Configure ExtremeNetworks.com Support

Allows the ability to request information about the latest Extreme Management Center product releases via the Help > Check for Updates option from the menu bar in any application and request information about firmware releases via the Help > Check for Firmware Updates option in Inventory Manager. It also allows you to configure the check for updates operation (including scheduled updates) in the Suite options. These features tell you when updated versions of Extreme Management Center products and firmware are available and allow you to download newer versions to keep your software and firmware current.

Configure Web Server

Allows the ability to specify the port ID for HTTP web server traffic.

Open GTAC Support Case

Allows the ability to create a GTAC support case or RMA case from the Network tab.

Server Information

View Server Information

Allows the ability to view, but not to configure the Server Information tool, accessed from the Tools menu in any Extreme Management Center application. Users who do not have this capability see an error message when they attempt to access the tool.

Configure Server View

Allows the ability to view and configure Extreme Management Center Console client connection options:

- View - Access and view the Client Connections Options window.
- Configure - Configure the type and number of clients that can connect to your server.

Extreme Management Center Database

Allows the following Extreme Management Center database management capabilities:

- View or Change Database Password - View and change the password the Extreme Management Center Server uses to access the database.
- Change Database URL - Change the URL the Extreme Management Center Server uses when connecting to the database.
- Backup Database - Save the currently active database to a file.
- Restore or Initialize Database - Restore the initial database or restore a saved database.
- Initialize Plugin Data - Initialize a specific Extreme Management Center application's components in the Extreme Management Center database by using the File > Database > Initialize Components menu option.

Disconnect Clients

Allows the ability to disconnect clients in the Client Connections tab and to configure the User Inactivity option in the Client Connections Suite-Wide options panel.

Revoke Locks

Allows the ability to revoke operation locks in the Locks tab.

Server Information

The Server Information tab lets you view and manage Extreme Management Center client connections and locks. You must be assigned the appropriate user capabilities to access and use this tab.

ZTP+ Registration

Allows the ability to configure a ZTP+ enabled device and add it to Extreme Management Center.

Northbound API

Extreme Management Center Northbound API Read Access

Allows the ability to access Extreme Management Center information from third-party integrations via an API.

Vendor Profiles

Extreme Management Center Vendor Profile Read Access

Allows the ability to view vendor profiles on the Administration tab in Extreme Management Center.

Extreme Management Center Vendor Profile Read/Write Access

Allows the ability to view and configure vendor profiles on the Administration tab in Extreme Management Center.

Workflows

Extreme Management Center Workflows Read Access

Allows the ability to view workflows on the Tasks tab in Extreme Management Center.

Extreme Management Center Workflows Read/Write Access

Allows the ability to view and edit workflows on the Tasks tab in Extreme Management Center.

NOTE: Access to some Extreme Management Center components is determined by capabilities in other capabilities groups:

NetSight (Extreme Management Center) Console > Wireless Manager > Launch
Adds the ability to view the Wireless tab.

NetSight (Extreme Management Center) Suite > Devices > Add, Discover and Import
Adds the ability to add devices in the Network tab.

NetSight (Extreme Management Center) Suite > Devices > Delete
Adds the ability to delete devices in the Network tab.

Inventory Manager > Configuration Archive Management > View/Compare Configurations
Adds the ability to compare archived device configurations in either the Network tab or the Archive Details Report available in the Reports tab.

Extreme Access Control Options

Selecting Extreme Access Control in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the **Control** > **Extreme Access Control** tab. The right-panel view changes depending on what you select in the left-panel tree. Expand the Extreme Access Control tree to view all the different available options. These settings apply to all users.

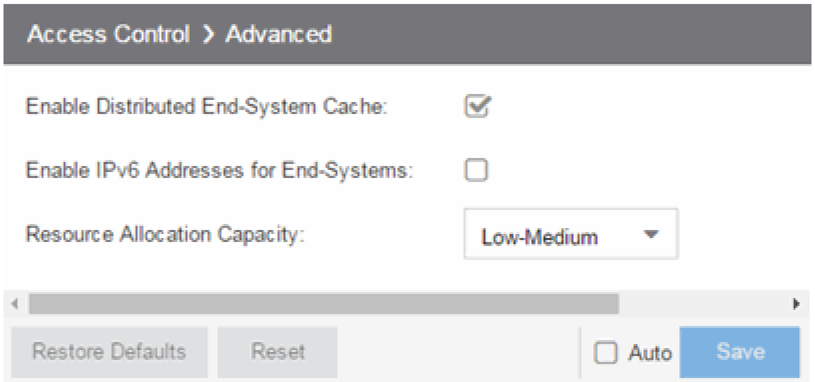
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Click the link for information on the following Extreme Access Control options:

- Advanced
- Assessment Server
- Data Persistence
- Display
- End-System Event Cache
- Enforce Warning Settings
- Features
- Notification Engine
- Policy Defaults
- Status Polling and Timeout

Advanced

This view lets you configure advanced settings for the **Extreme Access Control** tab.



Access Control > Advanced

Enable Distributed End-System Cache: ☑

Enable IPv6 Addresses for End-Systems: □

Resource Allocation Capacity: Low-Medium

Enable Distributed End-System Cache

The **Enable Distributed End-System Cache** option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling this option improves Extreme Access Control performance when discovering new end-systems as they connect, or when end-systems move from one place to another in the network.

To use the end-system cache feature, it must be enabled on both the Extreme Management Center Server (using this option) and on the Extreme Access Control engines using the cache.

When this feature is enabled, the Extreme Management Center Server and the Extreme Access Control engine exchange additional data each time end-system data is updated. This feature is **not** recommended unless there is sufficient network bandwidth for the additional data, a fast connection between the Extreme Management Center Server and the Extreme Access Control engine, and end-systems are adding or moving frequently.

Enable IPv6 Addresses for End-Systems

The **Enable IPv6 Addresses for End-Systems** option allows Extreme Access Control to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems need to rediscover their IP addresses in order to reflect the change in the end-systems table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system.

Only end-systems with a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems with only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see

IPv6 Support in the Extreme Management Center Configuration Considerations Help topic.

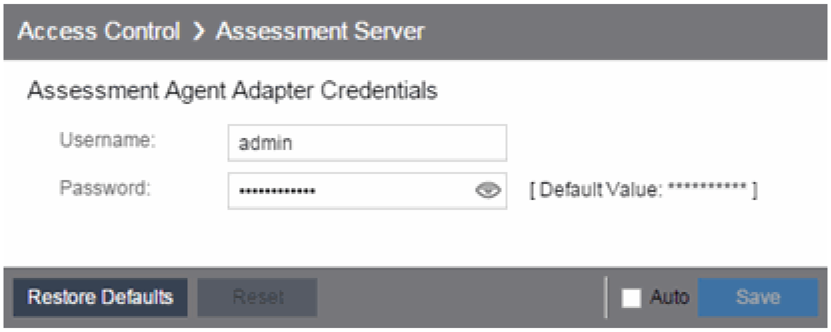
Resource Allocation Capacity

The **Resource Allocation Capacity** option lets you configure the Extreme Management Center resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Extreme Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

Assessment Server

These options let you provide assessment agent adapter credentials.



Access Control > Assessment Server

Assessment Agent Adapter Credentials

Username: admin

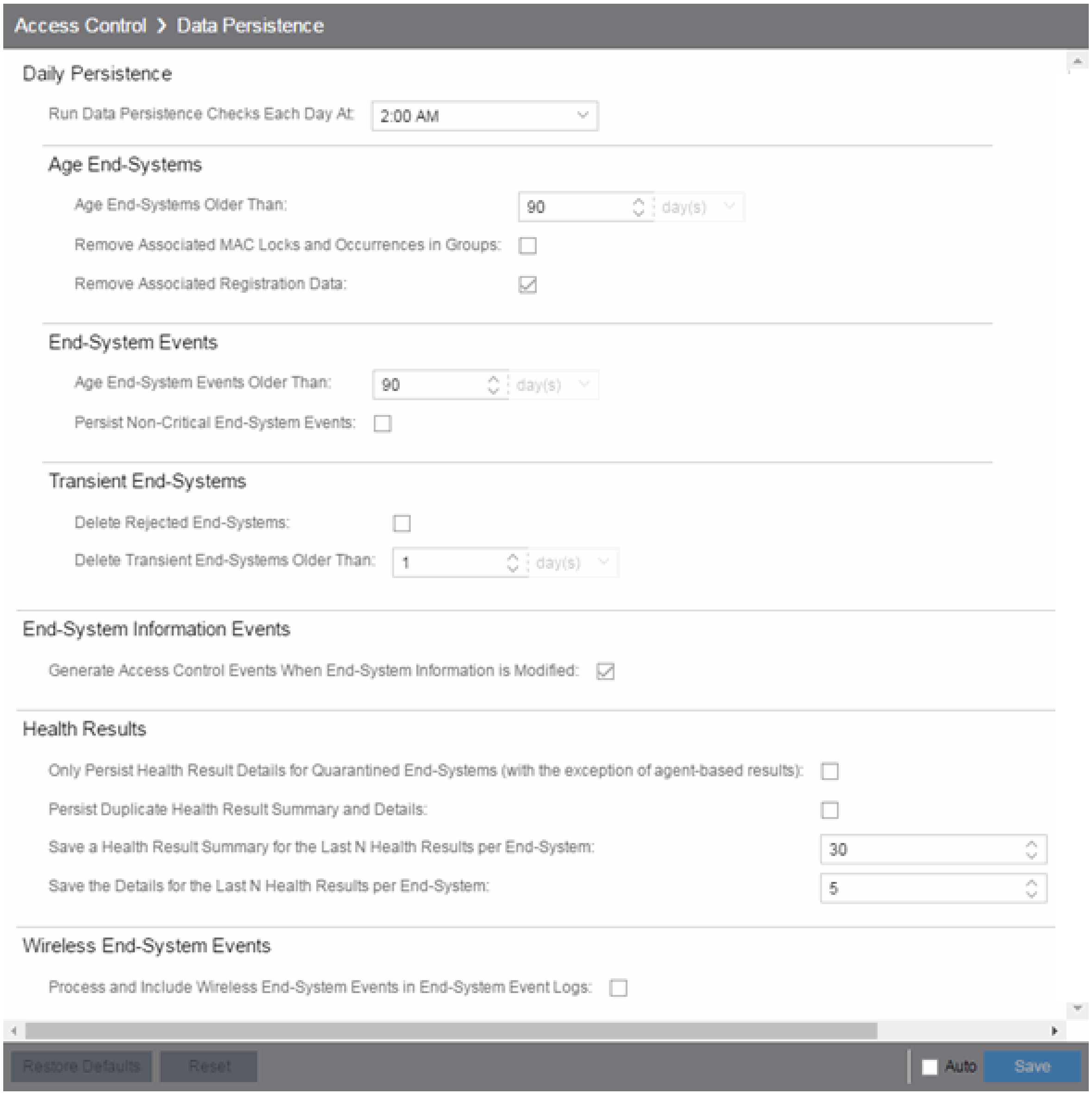
Password: ••••••••••••• [Default Value: ***********]

Assessment Agent Adapter Credentials

Specify the username and password the Extreme Access Control engine uses when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server not supplied or supported by Extreme Management Center). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. Extreme Management Center provides a default password you can change, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For additional information, see How to Change the Assessment Agent Adapter Password.

Data Persistence

This panel lets you customize how Extreme Access Control ages-out or deletes end-systems, end-system events, and end-system health (assessment) results from the tables and charts in the End-Systems view.



Daily Persistence

Run Data Persistence Checks Each Day At: 2:00 AM

Age End-Systems

Age End-Systems Older Than: 90 day(s)

Remove Associated MAC Locks and Occurrences in Groups: □

Remove Associated Registration Data: ☑

End-System Events

Age End-System Events Older Than: 90 day(s)

Persist Non-Critical End-System Events: □

Transient End-Systems

Delete Rejected End-Systems: □

Delete Transient End-Systems Older Than: 1 day(s)

End-System Information Events

Generate Access Control Events When End-System Information is Modified: ☑

Health Results

Only Persist Health Result Details for Quarantined End-Systems (with the exception of agent-based results): □

Persist Duplicate Health Result Summary and Details: □

Save a Health Result Summary for the Last N Health Results per End-System: 30

Save the Details for the Last N Health Results per End-System: 5

Wireless End-System Events

Process and Include Wireless End-System Events in End-System Event Logs: □

Daily Persistence

Run Data Persistence Checks Each Day At

Set the time that the Data Persistence Check is performed each day.

Age End-Systems

Age End-Systems Older Than

Specify the amount of time Extreme Management Center keeps end-system information in the database. Each day, when the Data Persistence check runs, it searches the database for end-systems for which Extreme Access Control did not receive an event in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the End-Systems tab.

If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

The **Remove Associated Registration Data** checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.

End-System Events

Age End-System Events Older Than

End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes all end-system events which are older than the number of days specified (90 days by default).

Persist Non-Critical End-System Events

Select this checkbox to save non-critical end-system events (e.g. duplicate end-system events, re-authentication events where the end-system's state did not change) to the database.

Transient End-Systems

Delete Rejected End-Systems

Select this checkbox to delete end-systems in the Rejected state as part of the cleanup.

Delete Transient End-Systems Older Than

Specify the amount of time to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are unregistered end-systems not seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them.

End-System Information Events

Generate Extreme Access Control Events When End-System Information is Modified

Select the checkbox if you want Extreme Access Control to generate an event when end-system information is modified.

Health Results

Only Persist Health Result Details for Quarantined End-Systems (with the exception of agent-based results)

Select this checkbox to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).

Persist Duplicate Health Result Summary and Details

Select this checkbox to save duplicate health result summaries and details. By default, duplicate health results obtained during a single scan interval are not saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database.

Save a Health Result Summary for the Last N Health Results per End-System

Specify how many health (assessment) result summaries are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system.

Save the Details for the Last N Health Results per End-System

Specify how many health (assessment) result details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves detailed information for the last five health results per end-system.

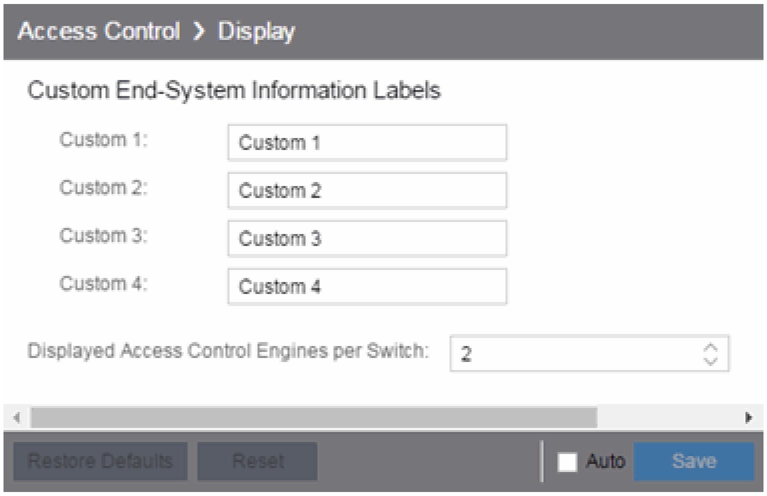
Wireless End-System Events

Process and Include Wireless End-System Events in End-System Event Logs

Select the checkbox if you want Extreme Management Center to generate an event when wireless end-system information is modified. This option is disabled by default.

Display

This Options view lets you configure new column names for the **Custom** columns in the End-System table on the **Control** > **End-Systems** tab, as well as the number of redundant Extreme Access Control Gateways you can select when adding or editing a switch in an Extreme Access Control Engine group.



Access Control > Display

Custom End-System Information Labels

Custom 1: Custom 1

Custom 2: Custom 2

Custom 3: Custom 3

Custom 4: Custom 4

Displayed Access Control Engines per Switch: 2

Custom End-System Information Labels

This option lets you specify new text for the **Custom** column headings in the End-System table on the **End-Systems** tab.

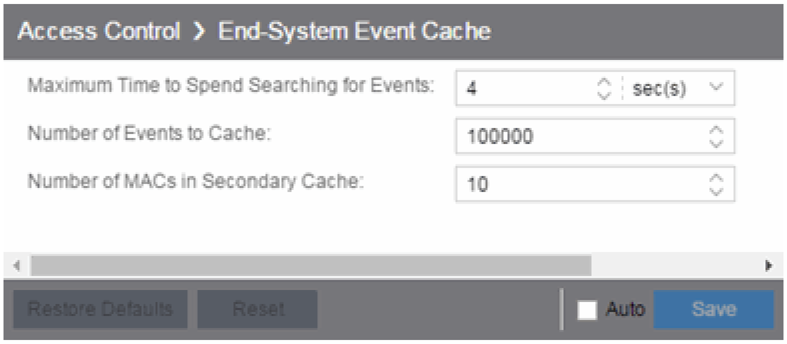
Displayed Extreme Access Control Engines per Switch

Select the number of Extreme Access Control engines displayed in the Add Switches to Group or Edit Switches in Group windows. By default, these windows allow you to configure two Extreme Access Control engines per switch for redundancy, but this option allows you to increase the number up to three or four engines per switch.

End-System Event Cache

End-system events are stored in the database. In addition, the end-system event cache stores the most recent end-system events in memory and displays them in the End-System Events tab. This cache allows Extreme Access Control to quickly retrieve and display end-system events without having to search through the database.

These options let you configure the amount of resources used by the end-system event cache.



Access Control > End-System Event Cache

Maximum Time to Spend Searching for Events: 4 sec(s)

Number of Events to Cache: 100000

Number of MACs in Secondary Cache: 10

Maximum Time to Spend Searching for Events

Specify the time Extreme Management Center spends when searching for older events outside of the cache. (The search is initiated by using the Search for Older Events button in the End-System Events tab.) The search is ended when the number of seconds entered is reached.

Number of Events to Cache

Specify the number of events to cache. The more events you cache, the faster data is returned, but caching uses more memory.

Number of MACs in Secondary Cache

The End-System Event Cache also keeps a secondary cache of events by MAC address. This means that a particular end-system's events can be more quickly accessed in subsequent requests. Use this field to specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note that the secondary cache may include events not in the main cache.

Enforce Warnings to Ignore

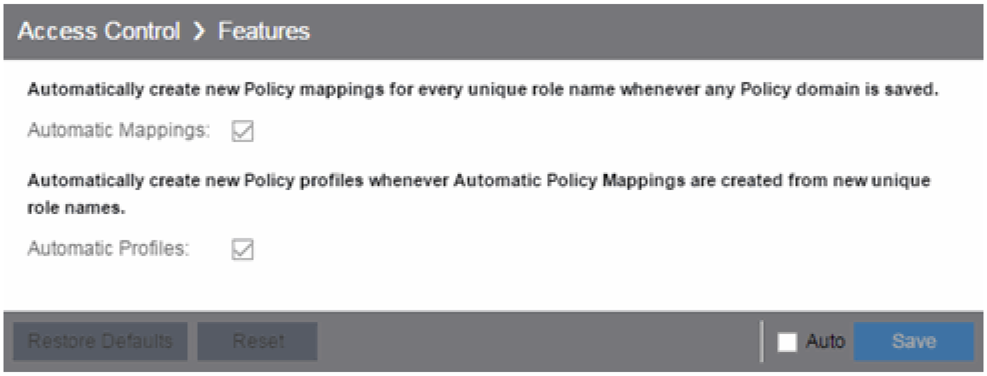
Select the checkbox next to the warning message you don't want displayed and click Save.

When an engine configuration audit is performed during an Enforce operation, warning messages may be displayed in the audit results listed in the Enforce window. If there is a warning associated with an engine, you are given the option to acknowledge the warning and proceed with the enforce anyway.

These settings allow you to select specific warning messages you do not want displayed in the audit results. This allows you to proceed with the Enforce without having to acknowledge the warning message. For example, your network always results in one of these warning messages on your Extreme Access Control configuration. By selecting that warning here, it is ignored in future audit results and you no longer need to acknowledge it before proceeding with the Enforce.

Features

This panel lets you automatically create new Policy mappings and profiles. If you are not using these features, disable them to remove sections that pertain only to those features from certain Extreme Access Control windows.



Access Control > Features

Automatically create new Policy mappings for every unique role name whenever any Policy domain is saved.

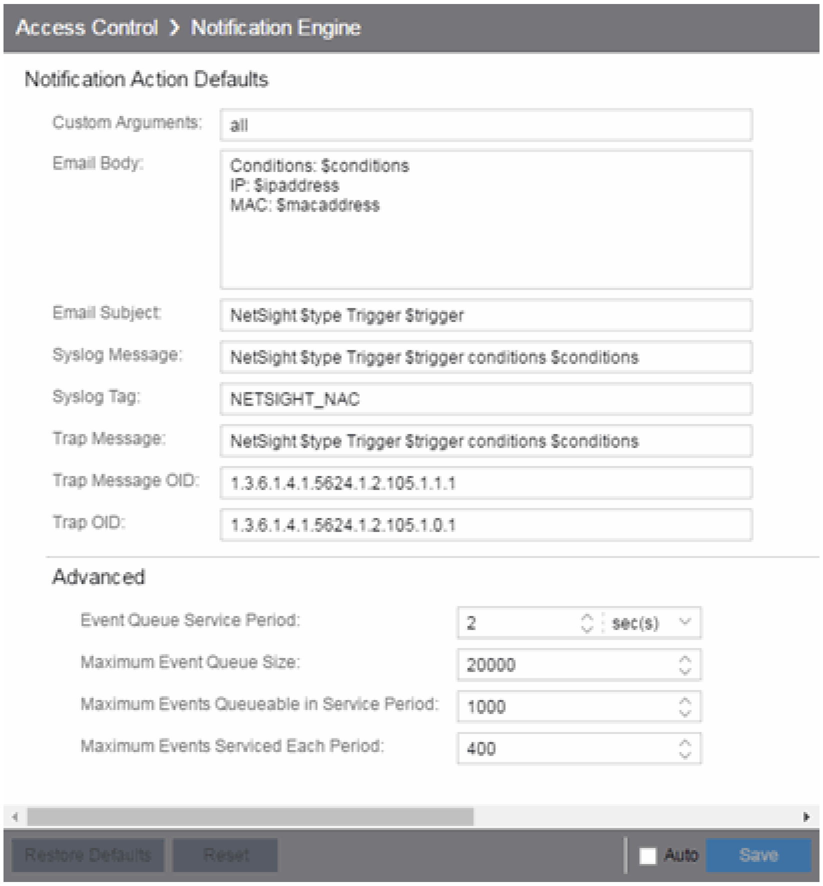
Automatic Mappings: ☑

Automatically create new Policy profiles whenever Automatic Policy Mappings are created from new unique role names.

Automatic Profiles: ☑

Notification Engine

This panel lets you define the default content contained in Extreme Access Control notification action messages. For example, with an email notification action, define the information contained in the email subject line and body. With a syslog or trap notification action, define the information included in the syslog or trap message.



Notification Action Defaults

Custom Arguments: all

Email Body:
Conditions: $conditions
IP: $ipaddress
MAC: $macaddress

Email Subject: NetSight $type Trigger $trigger

Syslog Message: NetSight $type Trigger $trigger conditions $conditions

Syslog Tag: NETSIGHT_NAC

Trap Message: NetSight $type Trigger $trigger conditions $conditions

Trap Message OID: 1.3.6.1.4.1.5624.1.2.105.1.1.1

Trap OID: 1.3.6.1.4.1.5624.1.2.105.1.0.1

Advanced

Event Queue Service Period: 2 sec(s)

Maximum Event Queue Size: 20000

Maximum Events Queueable in Service Period: 1000

Maximum Events Serviced Each Period: 400

There are certain "keywords" available to use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For additional information, see Keywords.

- $type - the notification type.
- $trigger - the notification trigger.
- $conditions - a list of the conditions specified in the notification action.
- $ipaddress - the IP address of the end-system that is the source of the event.
- $macaddress - the MAC address of the end-system that is the source of the event.
- $switchIP - the IP address of the switch where the end-system connected.
- $switchPort - the port number on the switch where the end-system connected.
- $username - the username provided by the end user upon connection to the network.

Custom Arguments

If the notification action specifies a custom program or script to be run on the Extreme Management Center Server, then use this field to enter the "all" option. Using the "all" option returns values for all the Extreme Access Control Notification keywords applicable to the notification type. For additional information, see Keywords.

Email Subject

Defines the text and keyword values included in the email subject line.

Email Body

Defines the text and keyword values included in the email body.

Syslog Message

Defines the text and keyword values included in the syslog message.

Syslog Tag

Defines the string used to identify the message issued by the syslog program.

Trap Message

The varbind sent in the trap.

Trap Message OID

The OID of the varbind being sent that represents the message.

Trap OID

The OID that defines the trap.

Event Queue Service Period

Defines how often the queue is checked for events to process. The dispatcher runs once every service period. So by default, the dispatcher processes events every 5 seconds.

Maximum Event Queue Size

The maximum number of events that can be queued. By default, the dispatcher drops events after 5000 events are queued.

Maximum Events Queuable in Service Period

This limits the rate that events can be added to the queue (not processed from the queue) and protects the event engine against a large amount of events arriving too quickly. If events arrive at a rate that exceeds this amount, they are discarded.

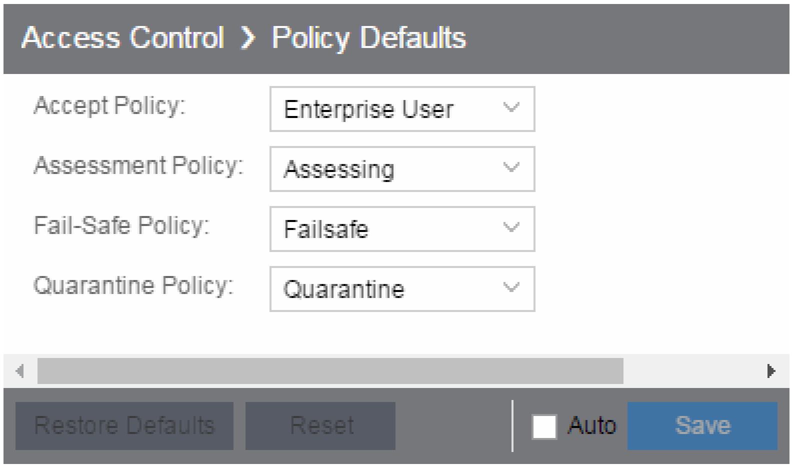
Maximum Events Serviced Each Period

The maximum number of events pulled from the queue for processing each service period. By default, the dispatcher processes 100 events every service period.

Policy Defaults

This Options view lets you specify a default policy for each of the four access policies. These default policies display as the first selection in the drop-down menus when you create an Extreme Access Control profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" is automatically displayed as the first selection in the Assessment Policy drop-down menu in the New Extreme Access Control Profile window.

Extreme Management Center supplies seven policy names from which you can select. Add more policies in the Edit Policy Mapping window, where you can also define policy to VLAN associations for RFC 3580-enabled switches. Once a policy is added, it becomes available for selection in this view.



Access Control > Policy Defaults

Accept Policy: Enterprise User

Assessment Policy: Assessing

Fail-Safe Policy: Failsafe

Quarantine Policy: Quarantine

Accept Policy

Select the default Accept policy. The Accept policy is applied to an end-system when the end-system is authorized locally by the Extreme Access Control engine and passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option is used when authenticating the end-system.

Assessment Policy

Select the default Assessment policy. The Assessment policy is applied to an end-system while it is being assessed (scanned).

Fail-Safe Policy

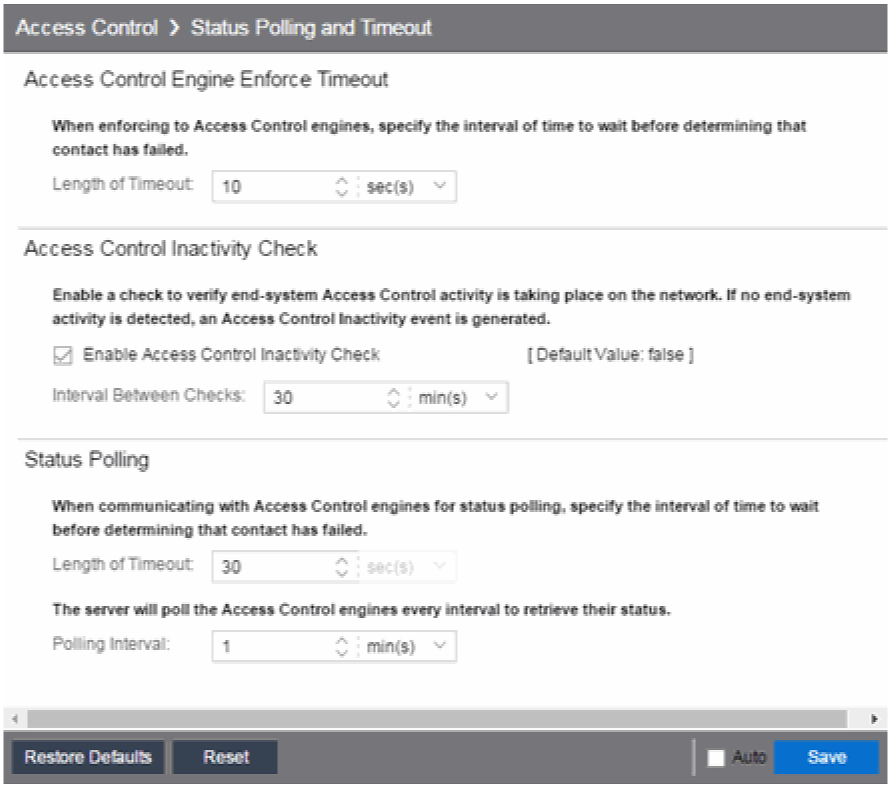
Select the default fail-safe policy. The fail-safe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there is a scanning error and an assessment of the end-system could not take place.

Quarantine Policy

Select the default Quarantine policy. The Quarantine policy is applied to an end-system if the end-system fails an assessment.

Status Polling and Timeout

This Options panel lets you specify the enforce timeout and status polling options for Extreme Access Control engines.



Access Control > Status Polling and Timeout

Access Control Engine Enforce Timeout

When enforcing to Access Control engines, specify the interval of time to wait before determining that contact has failed.

Length of Timeout: 10 sec(s)

Access Control Inactivity Check

Enable a check to verify end-system Access Control activity is taking place on the network. If no end-system activity is detected, an Access Control Inactivity event is generated.

☑ Enable Access Control Inactivity Check [Default Value: false]

Interval Between Checks: 30 min(s)

Status Polling

When communicating with Access Control engines for status polling, specify the interval of time to wait before determining that contact has failed.

Length of Timeout: 30 sec(s)

The server will poll the Access Control engines every interval to retrieve their status.

Polling Interval: 1 min(s)

□ Auto

Extreme Access Control Engine Enforce Timeout

When enforcing to Extreme Access Control engines, this value specifies the amount of time Extreme Management Center waits for an enforce response from the engine before determining the engine is not responding. During an enforce, an Extreme Access Control engine responds every second to report that the enforce operation is either in-progress or complete. Do not increase this timeout value, unless you are experiencing network delays that require a longer timeout value.

Extreme Access Control Inactivity Check

Enable a check to verify end-system Extreme Access Control activity is taking place on the network. If no end-system activity is detected, an Extreme Access Control Inactivity event is sent to the Events view. Use the Alarms and Events tab to configure custom alarm criteria based on the Extreme Access Control Inactivity event to create an alarm, if desired.

Status Polling

Length of Timeout — When communicating with Extreme Access Control engines for status polling, this value specifies the amount of time Extreme Management Center waits before determining contact failed. If Extreme Management Center does not receive a response from an engine in the defined amount of time, Extreme Management Center considers the engine to be "down". The engine status refers to Messaging connectivity, not SNMP connectivity. This means that if the engine is "down," Extreme Management Center is not able to enforce a new configuration to it.

Polling Interval — Specifies the frequency Extreme Management Center polls the Extreme Access Control engines to determine engine status.

Related Information

For information on related topics:

- Extreme Access Control

Alarm Options

Selecting Alarm in the left panel of the **Options** tab provides the following view, where you can configure alarm settings.

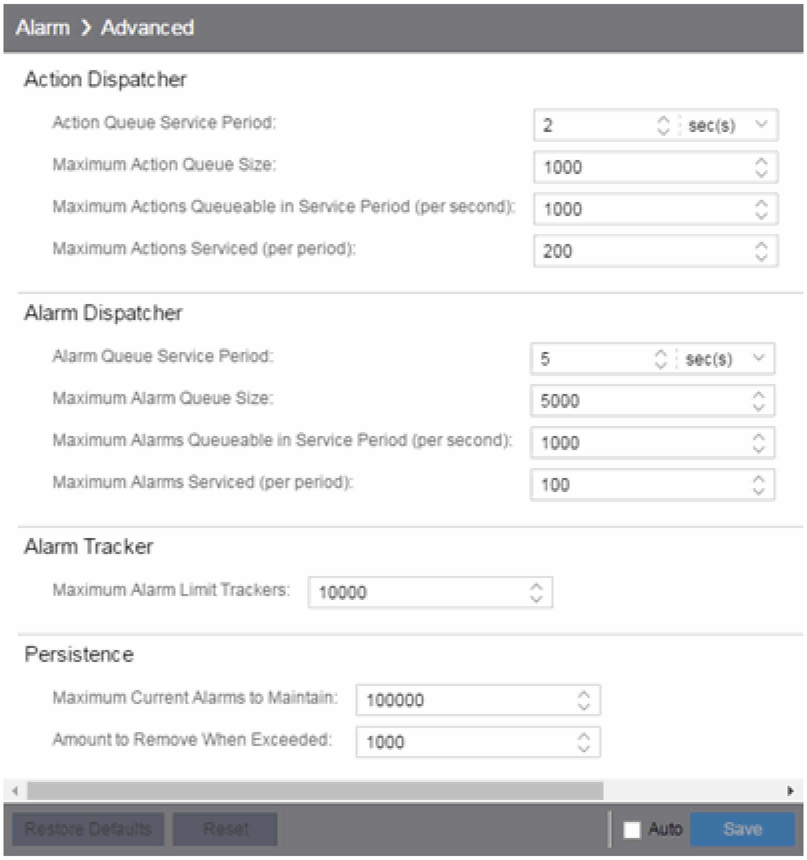
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Click the link for information on the following Alarm options:

- Advanced
- Alarm Action Defaults
- Alarm History
- Consolidate Email
- Override Email

Advanced

This view lets you configure advanced settings for the alarms functionality in Extreme Management Center. These settings apply to all users.



Alarm > Advanced

Action Dispatcher

Action Queue Service Period: 2 sec(s)

Maximum Action Queue Size: 1000

Maximum Actions Queueable in Service Period (per second): 1000

Maximum Actions Serviced (per period): 200

Alarm Dispatcher

Alarm Queue Service Period: 5 sec(s)

Maximum Alarm Queue Size: 5000

Maximum Alarms Queueable in Service Period (per second): 1000

Maximum Alarms Serviced (per period): 100

Alarm Tracker

Maximum Alarm Limit Trackers: 10000

Persistence

Maximum Current Alarms to Maintain: 100000

Amount to Remove When Exceeded: 1000

Action Dispatcher Options

Use these options to limit resources used by Extreme Management Center action handling.

After alarms are processed by the alarm dispatcher, they are checked for an action. If an action is found, the alarm is moved into the action queue for processing by the action dispatcher. A specified number of actions are taken from the queue and processed once each service period, according to the option values specified below.

Action Queue Service Period

This controls how often the queue is checked for actions to process. The dispatcher runs once every service period. So by default, the dispatcher processes actions every 2 seconds.

Maximum Action Queue Size

The maximum number of actions that can be queued. By default, the dispatcher drops actions after 1,000 actions are queued.

Maximum Actions Queuable in Service Period (per second)

This limits the rate at which actions can be added to the queue (not processed from the queue) and protects the alarm engine against a large amount of actions arriving too quickly. If actions arrive at a rate that exceeds this amount, they are discarded.

Maximum Actions Serviced (per period)

The maximum number of actions pulled from the queue for processing each service period. By default, the dispatcher processes 200 actions every service period.

Alarm Dispatcher Options

Use these options to limit resources used by Extreme Management Center alarm handling.

When alarms are triggered, they are moved into the alarm queue for processing by the alarm dispatcher. A specified number of alarms are taken from the queue and processed once each service period, according to the option values specified below.

Alarm Queue Service Period

This controls how often the queue is checked for alarms to process. The dispatcher runs once every service period, so by default, the dispatcher processes alarms every 5 seconds.

Maximum Alarm Queue Size

The maximum number of alarms that can be queued. By default, the dispatcher drops alarms after 5,000 alarms are queued.

Maximum Alarms Queuable in Service Period (per second)

This limits the rate at which alarms can be added to the queue (not processed from the queue) and protects the alarm engine against a large amount of alarms arriving too quickly. If alarms arrive at a rate that exceeds this amount, they are discarded.

Max Alarms Serviced (per period)

The maximum number of alarms pulled from the queue for processing each service period. By default, the dispatcher processes 100 alarms every service period.

Alarm Tracker Options

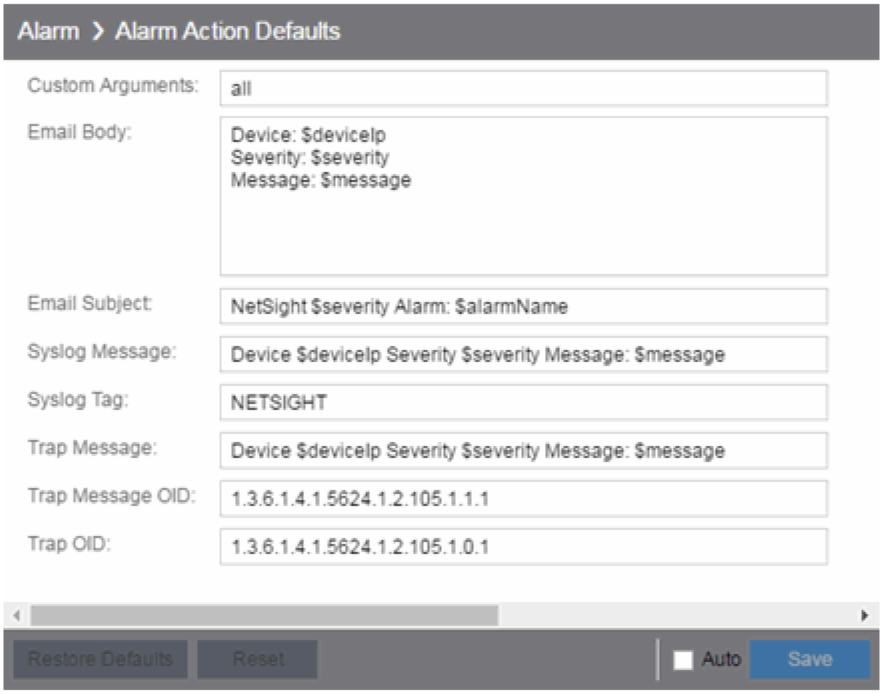
When you define an alarm with a limit, Extreme Management Center tracks whether the limit is exceeded and when to reset the count. This option sets the maximum number of alarms that Extreme Management Center tracks. (An alarm limit specifies the number of times the alarm action performed for an alarm.)

Increase the number if you are sure the system is able to handle the increased load.

Persistence Options

Use these options to prevent or troubleshoot Extreme Management Center performance problems caused by the number of current alarms being maintained. If you increase the maximum number of current alarms to maintain, be sure the server system is able to handle the increased load. Only increase the number of alarms to remove if the maximum current alarms number is being exceeded too frequently.

Alarm Action Defaults



Alarm > Alarm Action Defaults

Custom Arguments:	all
Email Body:	Device: $deviceIp Severity: $severity Message: $message
Email Subject:	NetSight $severity Alarm: $alarmName
Syslog Message:	Device $deviceIp Severity $severity Message: $message
Syslog Tag:	NETSIGHT
Trap Message:	Device $deviceIp Severity $severity Message: $message
Trap Message OID:	1.3.6.1.4.1.5624.1.2.105.1.1.1
Trap OID:	1.3.6.1.4.1.5624.1.2.105.1.0.1

Use this panel to define the default content for alarm action messages. For example, with an email action, define the information contained in the email subject line and body. With a syslog or trap action, specify the information you want contained in the syslog or trap message. These values are used unless they are overridden in an individual alarm.

The message content is configured as a template, with the content passed exactly as typed, except for the variable information which is specified by $keyword. The variable information ($keyword) is replaced with information from the alarm when the alarm action is executed.

Following is a list of the most common keywords used. For additional information, see Keywords.

- $alarmName – the name of the alarm.
- $severity – the severity of the alarm.
- $deviceIP – the IP address of the device that is the source of the alarm.
- $message – the event message.
- $time – the date and time when the event or trap occurred.

Custom Arguments

Specifies the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as $keyword. A group of literals and variables can be combined into a single argument by using double quotes. "All" is a special value that tells Extreme Management Center to pass all variable values to the program as individual arguments.

Email Body

Defines the text included in the email body.

Email Subject

Defines the text included in the email subject line.

Syslog Message

Defines the text included in the syslog message.

Syslog Tag

Defines the string used to identify the message issued by the syslog program.

Trap Message

The varbind sent in the trap.

Trap Message OID

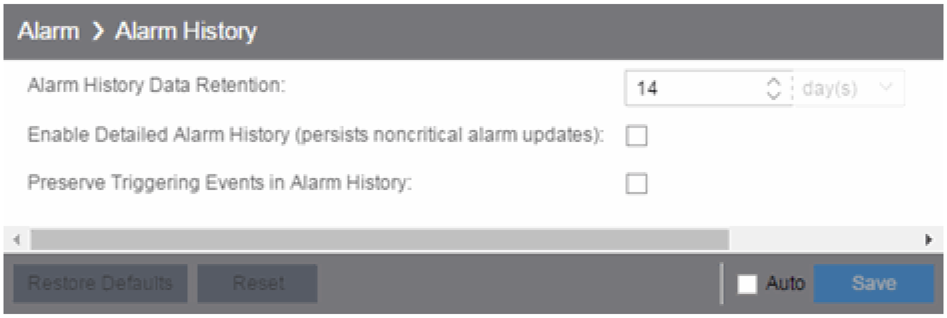
The OID of the varbind being sent that represents the message.

Trap OID

The OID that defines the trap.

Alarm History

Use this panel to configure options for how alarms are handled on your network. These settings apply to all users.



Alarm History Data Retention: 14 day(s)

Enable Detailed Alarm History (persists noncritical alarm updates): □

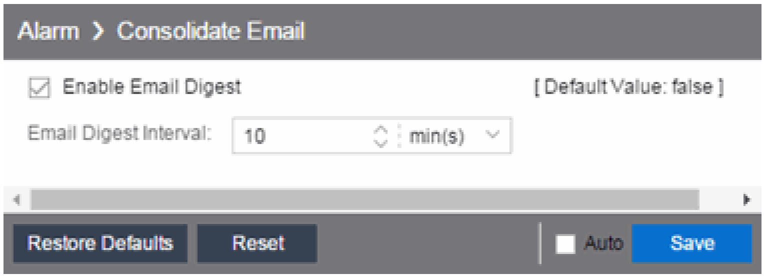
Preserve Triggering Events in Alarm History: □

Alarm History Data Retention
: Specify (in days) the amount of time Alarm History is retained.

Enable Detailed Alarm History (persists noncritical alarm updates)
: Select this checkbox to record repeat occurrences of an alarm being raised. By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared.

Preserve Triggering Events in Alarm History
: Select this checkbox to preserve alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by clicking the View Trigger button in the Alarm History window.

Consolidate Email



☑ Enable Email Digest [Default Value: false]

Email Digest Interval: 10 min(s)

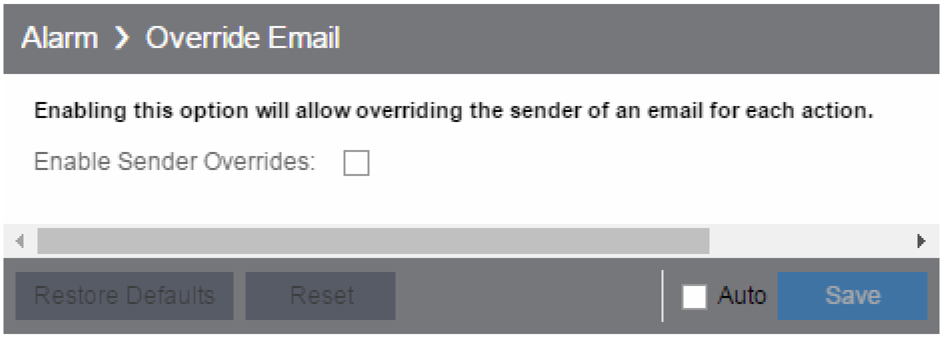
Enable Email Digest

Selecting this option combines alarm action emails into a single email. Email notifications are collected over the specified interval indicated in the **Email Digest Interval** and then delivered as a single consolidated email.

Email Digest Interval

Enter the amount of time Extreme Management Center waits before sending an email of alarm actions when **Select Enable Email Digest** is selected.

Override Email


Alarm > Override Email

Enabling this option will allow overriding the sender of an email for each action.

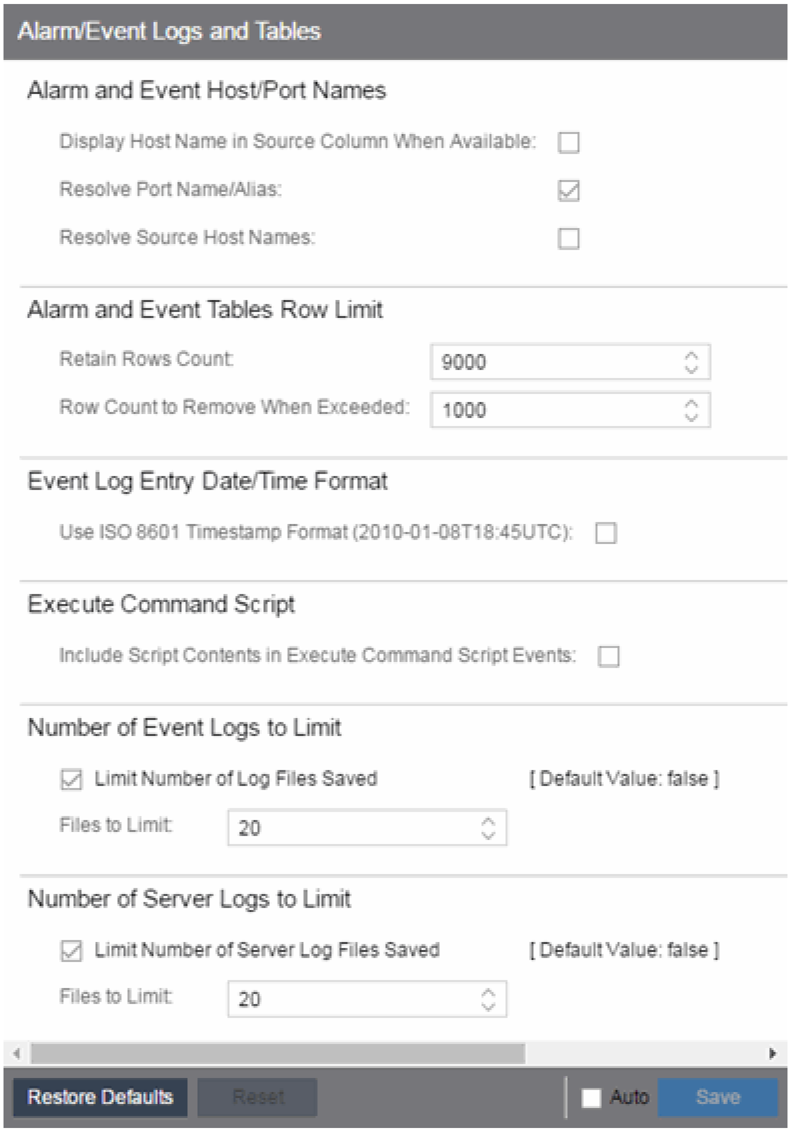
Enable Sender Overrides: □

Selecting this option allows you to override the sender of an email for an alarm email action, including the ability to set the sender's password, if needed. Since alarms are typically sent out as email/text messages, this option allows IT staff to set different ring-tones based on the alarm definition. Doing this on a smartphone typically involves changing the ring-tone for calls from a specific person.

Alarm/Event Logs and Tables Options

Selecting Alarm/Event Logs and Tables in the left panel of the **Options** tab provides the following view, where you can specify options for limiting disk usage by alarm and event logs, and Extreme Management Center server logs. These settings apply to all users. You must be assigned the appropriate user capability to configure these options. For additional information, see Extreme Management Center Log Files.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Alarm/Event Logs and Tables

Alarm and Event Host/Port Names

Display Host Name in Source Column When Available: □

Resolve Port Name/Alias: ☑

Resolve Source Host Names: □

Alarm and Event Tables Row Limit

Retain Rows Count: 9000

Row Count to Remove When Exceeded: 1000

Event Log Entry Date/Time Format

Use ISO 8601 Timestamp Format (2010-01-08T18:45UTC): □

Execute Command Script

Include Script Contents in Execute Command Script Events: □

Number of Event Logs to Limit

☑ Limit Number of Log Files Saved [Default Value: false]

Files to Limit: 20

Number of Server Logs to Limit

☑ Limit Number of Server Log Files Saved [Default Value: false]

Files to Limit: 20

Alarm and Event Host/Port Names

These options let you configure host name and port name resolution, and display the device host name in the Source column in alarm and event tables:

- Display Host Name in Source Column When Available — Select this option to display the host name in the source column on both the Alarms and Events tabs of the Alarms and Events tab, if it's available in Extreme Management Center.
- Resolve Port Name/Alias — Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to enable/disable port name resolution for Event and Alarm tables only. (Port name resolution is enabled globally using the Enable Name Resolution option.)
- Resolve Source Host Names — Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to enable/disable host name resolution for the Event and Alarm tables only. (Host name resolution is enabled globally using the Enable Name Resolution option.)

Alarm and Event Tables Row Limit

These settings determine the number of table rows displayed in all of the logs on both the Alarms and Events tabs of the Alarms and Events tab. The table size reaches an absolute limit when the number of rows is equal to the value in the Retain Rows Count field. When the number of rows exceeds that value, the number of rows are reduced by the value specified in the Row Count to Remove When Exceeded field. Subsequent entries are retained until the Retain Rows Count value is exceeded and the row total is again reduced.

Event Log Entry Date/Time Format

This option lets you specify the timestamp format used for log entries in the actual application log files. (This option does not affect the log entry format displayed in Extreme Management Center client Event Log views.) Selecting Use ISO 8601 Timestamp Format displays log entry timestamps in a readable format that makes it easier to view the files in a text file. Not selecting this option uses the raw timestamp format, in which timestamps are displayed in a raw, non-readable format.

Execute Command Script

The Execute Command Script feature includes script contents in logged events, which is not secure if the script includes passwords. If this option is deselected (default), the script is removed from the logged event. Select this option to include script contents in Execute Command Script events.

Number of Event Logs to Limit

This option limits the number of application log files saved to the `<install directory>\appdata\logs` directory. It does not limit the number of Traps or Syslog log files saved.

- Limit Number of Log Files Saved — Selecting the checkbox sets a limit to the number of application log files saved. Older files are deleted when the maximum number is reached.
- Files to Limit — Enter the maximum number of application log files saved.

Number of Server Logs to Limit

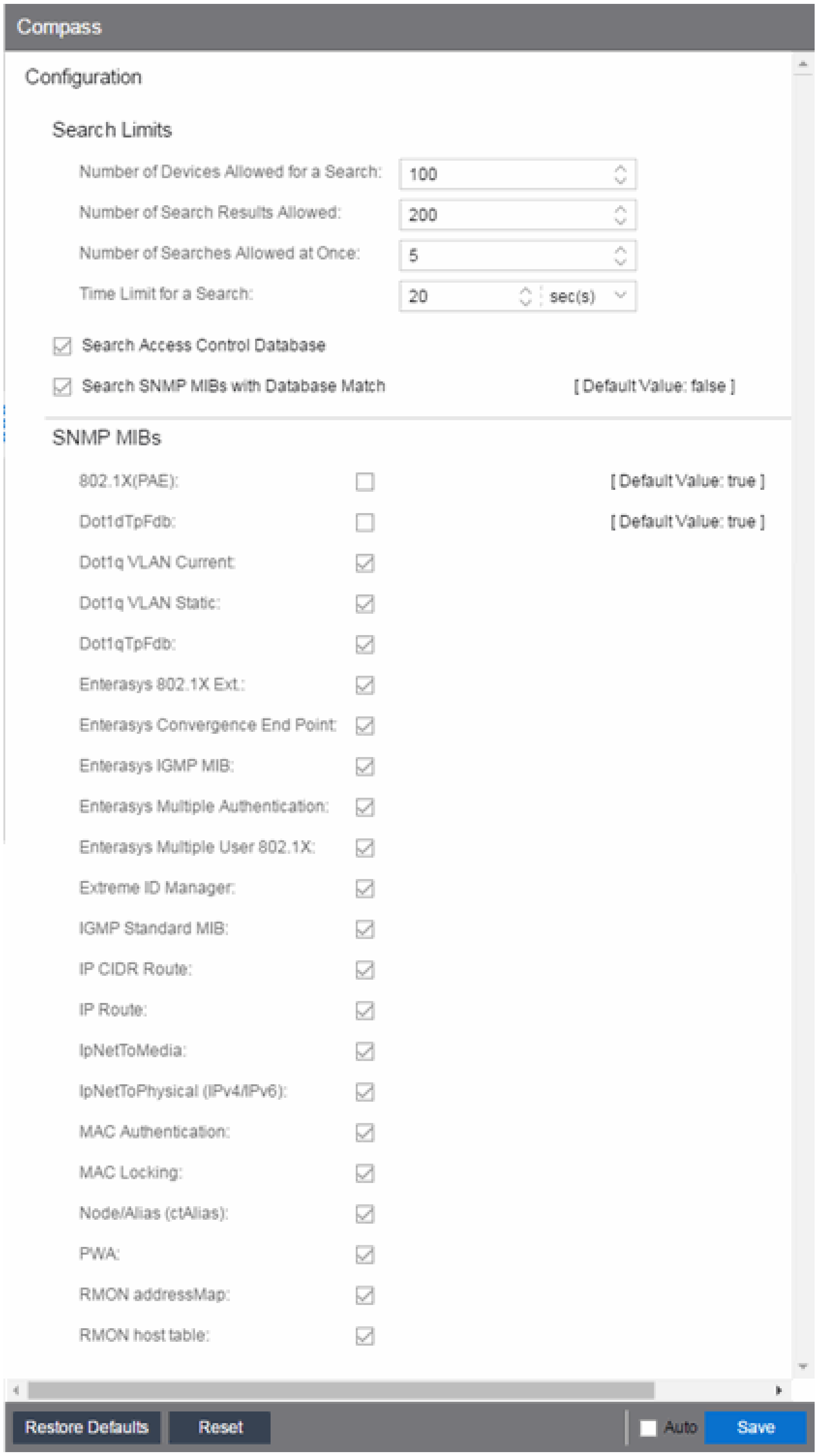
A new server log is created every day. This option limits the number of server log files that are saved to the `<install directory>\appdata\logs` directory.

- Limit Number of Server Log Files Saved — Selecting the checkbox sets a limit to the number of server log files saved. Older files are deleted when the maximum number is reached.
- Files to Limit — Enter the maximum number of server log files saved.

Compass Options

Selecting Compass in the left panel of the **Options** tab provides the following view, where you can specify Compass SNMP and Search options.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Compass

Configuration

Search Limits

Number of Devices Allowed for a Search: 100

Number of Search Results Allowed: 200

Number of Searches Allowed at Once: 5

Time Limit for a Search: 20 sec(s)

☑ Search Access Control Database

☑ Search SNMP MIBs with Database Match [Default Value: false]

SNMP MIBs

802.1X(PAE):	□	[Default Value: true]
Dot1dTpFdb:	□	[Default Value: true]
Dot1q VLAN Current:	☑	
Dot1q VLAN Static:	☑	
Dot1qTpFdb:	☑	
Enterasys 802.1X Ext.:	☑	
Enterasys Convergence End Point:	☑	
Enterasys IGMP MIB:	☑	
Enterasys Multiple Authentication:	☑	
Enterasys Multiple User 802.1X:	☑	
Extreme ID Manager:	☑	
IGMP Standard MIB:	☑	
IP CIDR Route:	☑	
IP Route:	☑	
IpNetToMedia:	☑	
IpNetToPhysical (IPv4/IPv6):	☑	
MAC Authentication:	☑	
MAC Locking:	☑	
Node/Alias (ctAlias):	☑	
PWA:	☑	
RMON addressMap:	☑	
RMON host table:	☑	

Search Limits

These options are for the Compass search in Extreme Management Center. In addition to search options, they include search limit settings, which are used to help limit the Extreme Management Center server resources used for the searches.

- Number of Devices Allowed for a Search — The maximum number of devices that can be included in a search.
- Number of Search Results Allowed — The maximum number of search results that can be displayed in the table.
- Number of Searches Allowed at Once — The maximum number of Extreme Management Center Compass searches that can be performed at one time.
- Time Limit for a Search — The maximum search time.

Search Extreme Access Control Database

Select this checkbox to include Extreme Access Control data in Compass searches. The Compass search begins by resolving IP address to MAC address in order to start searching for MAC-IP pairs from the network. When a match is found in the Extreme Access Control Database, the SNMP MIBs are not searched unless the Search SNMP MIBs with Database Match checkbox is also selected. If the Extreme Access Control checkbox is deselected, then the Extreme Access Control Database is not used to resolve IP address to MAC address.

Search SNMP MIBs with Database Match

Select this checkbox to include various SNMP MIB objects when performing searches. When the checkbox is selected, the SNMP MIBs section displays, from which you can select the individual SNMP MIB objects to include in Compass searches. For additional information, see Compass SNMP MIBs Descriptions.

Related Information

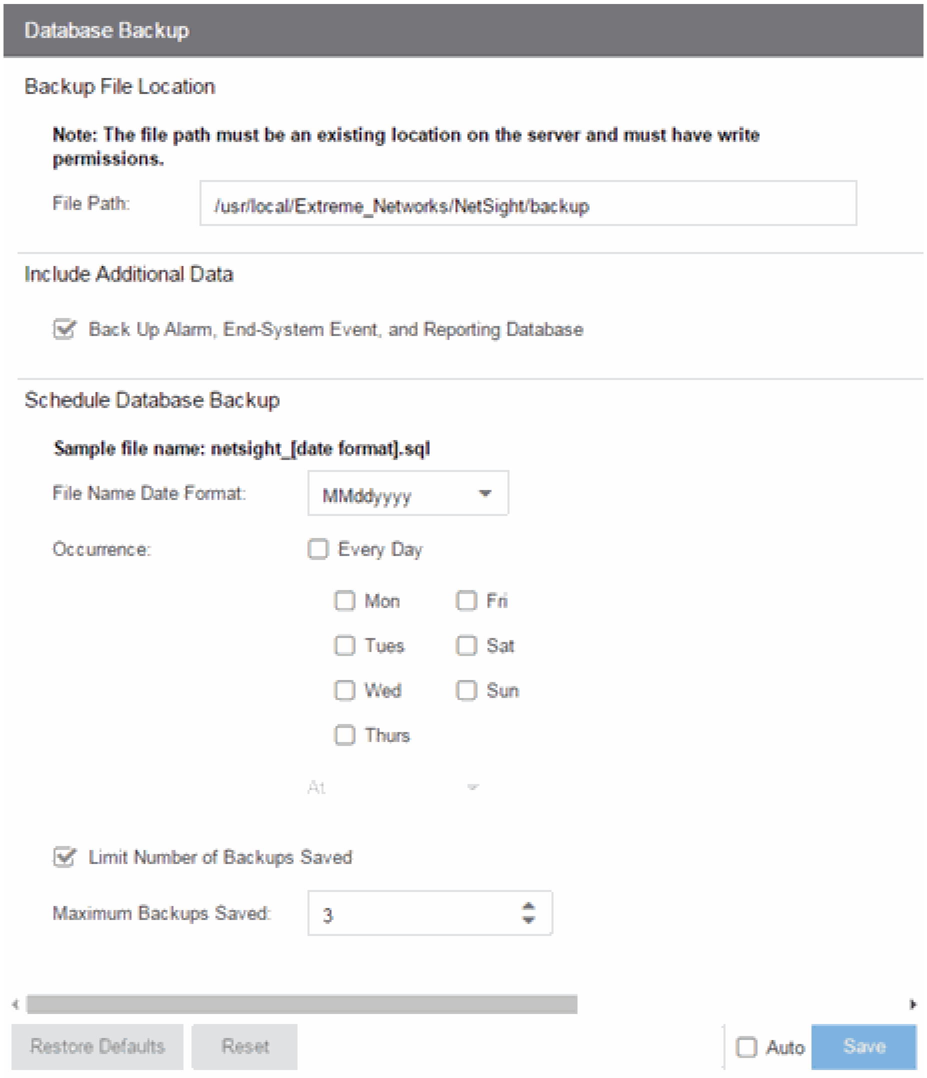
For information on related tasks:

- How to Set Extreme Access Control Options

Database Backup Options

Selecting Database Backup in the left panel of the **Options** tab provides the following view, where you can schedule backups of the Extreme Management Center database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all Extreme Management Center applications is saved and readily available, if needed.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Database Backup

Backup File Location

Note: The file path must be an existing location on the server and must have write permissions.

File Path: /usr/local/Extreme_Networks/NetSight/backup

Include Additional Data

☑ Back Up Alarm, End-System Event, and Reporting Database

Schedule Database Backup

Sample file name: netsight_[date format].sql

File Name Date Format: MMddyyyy

Occurrence: □ Every Day

□ Mon □ Fri
□ Tues □ Sat
□ Wed □ Sun
□ Thurs

At

☑ Limit Number of Backups Saved

Maximum Backups Saved: 3

Backup File Location

File Path

The database backup is saved to the directory specified in the File Path field. Saving backups to a separate location such as a network share ensures that an up-to-date copy of the database is available should a problem such as a server disk failure occur. The backup directory must exist and be writable or it is not accepted. Both the start and stop of the database backup are logged to the Console Event View log for verification and tracking purposes.

Include Additional Data

Back Up Alarm, End-System Event, and Reporting Database

This checkbox lets you enable and disable the automatic backup of alarm data, end-system event data, and Extreme Management Center reporting data. Because the alarm, event, and reporting databases can be quite large, this allows you to control the amount of disk space used by the database backup operation.

Schedule Database Backup

File Name Date Format

Customize the date and time formats of scheduled backup files by selecting the option that formats the date -- day (DD), month (MM), and year (YYYY) -- according to your personal preference in the drop-down menu.

Occurrence

Select one or more days of the week and specify a time for the backup to be performed. The backup takes place at the same time for each selected day.

Limit Number of Backups Saved

Select the checkbox to limit the number of scheduled backup files saved.

Maximum Backups Saved

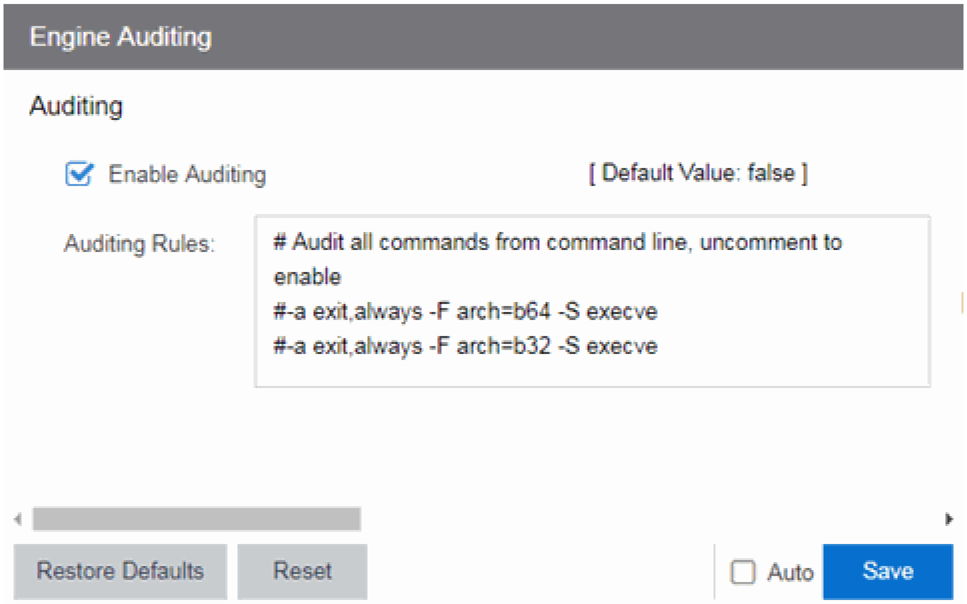
If Limit Number of Backups Saved is selected, enter the maximum number of scheduled backup files to save. When the limit is reached, older backups are removed when a new scheduled backup completes.

For additional information, see Tuning Database Backup Storage.

Engine Auditing Options

Selecting Engine Auditing in the left panel of the **Options** tab provides the following view, where you can enable auditing of users connected to the Extreme Management Center server CLI via SSH.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Engine Auditing

Auditing

☑ Enable Auditing [Default Value: false]

Auditing Rules:

```
# Audit all commands from command line, uncomment to enable
#-a exit,always -F arch=b64 -S execve
#-a exit,always -F arch=b32 -S execve
```

Enable Auditing

Selecting the **Enable Auditing** option enables the **Auditing Rules** field, where you can configure Extreme Management Center to store all commands entered by users connected to the Extreme Management Center CLI via SSH in the syslog file.

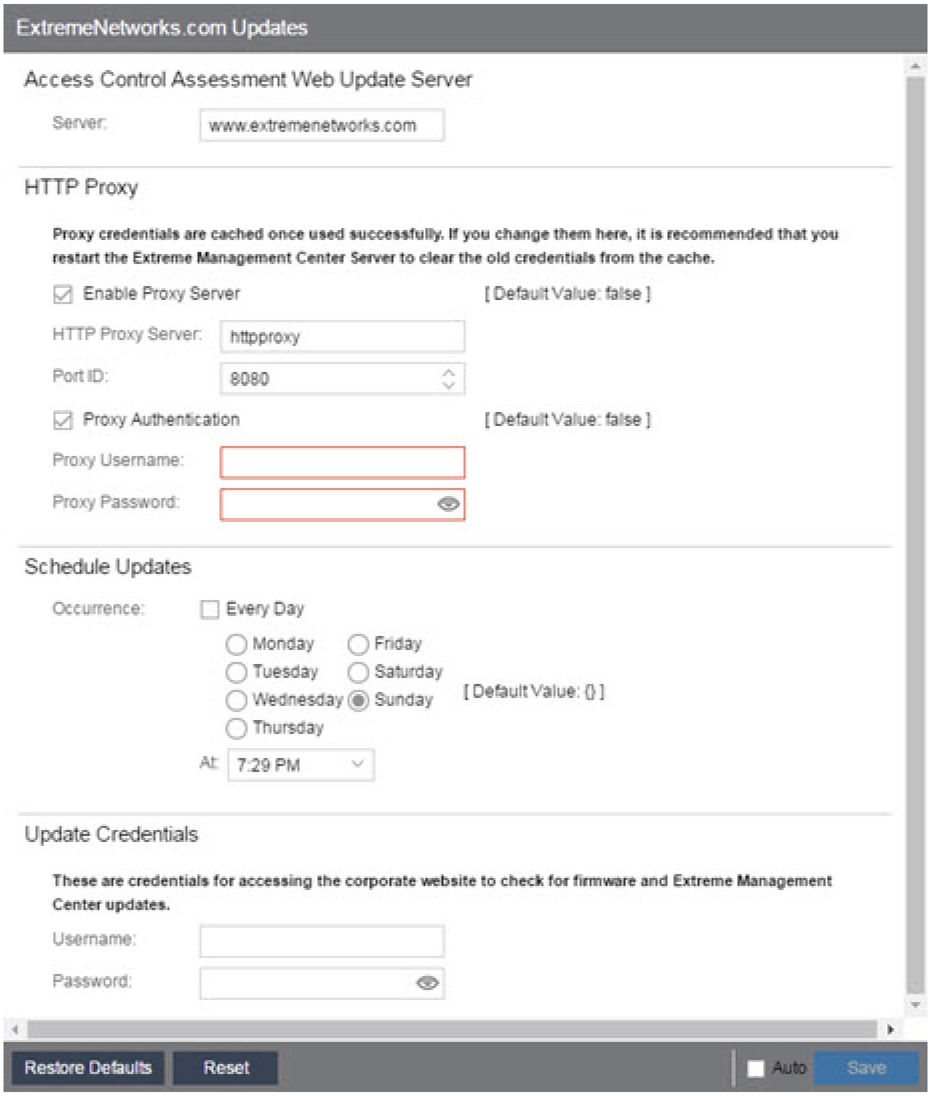
Auditing Rules

Remove the # symbol from the beginning of a command line to enable the command and store user commands entered using the Extreme Management Center CLI.

ExtremeNetworks.com Updates Options

Selecting ExtremeNetworks.com Updates in the left panel of the **Options** tab provides the following view, where you can configure options for accessing the ExtremeNetworks.com website to obtain information about the latest Extreme Management Center product releases and Extreme Networks firmware releases available for download. These settings apply to all users. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



ExtremeNetworks.com Updates

Access Control Assessment Web Update Server

Server: www.extremenetworks.com

HTTP Proxy

Proxy credentials are cached once used successfully. If you change them here, it is recommended that you restart the Extreme Management Center Server to clear the old credentials from the cache.

☑ Enable Proxy Server [Default Value: false]

HTTP Proxy Server: httpproxy

Port ID: 8080

☑ Proxy Authentication [Default Value: false]

Proxy Username:

Proxy Password:

Schedule Updates

Occurrence: □ Every Day

○ Monday ○ Friday
○ Tuesday ○ Saturday
○ Wednesday ● Sunday [Default Value: {}]
○ Thursday

At: 7:29 PM

Update Credentials

These are credentials for accessing the corporate website to check for firmware and Extreme Management Center updates.

Username:

Password:

Extreme Access Control Assessment Web Update Server

Displays the web update server used by Extreme Access Control to update Extreme Access Control assessment server software. This update operation pertains only to Extreme Access Control on-board agent-less assessment servers.

HTTP Proxy Server

If your network is protected by a firewall, select the **Enable Proxy Server** checkbox and enter your proxy server address and port ID. Consult your network administrator for this information. If your proxy server requires authentication, select the **Proxy Authentication** checkbox and enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server. Proxy credentials are cached once used successfully. If you change them here, restart the Extreme Management Center Server to clear the old credentials from the cache.

NOTE: The update procedure uses these proxy settings only when necessary; otherwise, the settings are ignored.

Schedule Updates

This section lets you schedule when Extreme Management Center checks for software updates:

- To check for updates every day — Select the **Every Day** checkbox, then select the time to run the check in the **At** drop-down menu.
- To check for updates once a week — Select the radio button that corresponds to the day of the week on which you want to run the check, then select the time to run the check in the **At** drop-down menu.
- To disable scheduled updates — Do not select the **Every Day** checkbox or any of the radio buttons or click the **Default Value** button to clear your selection.

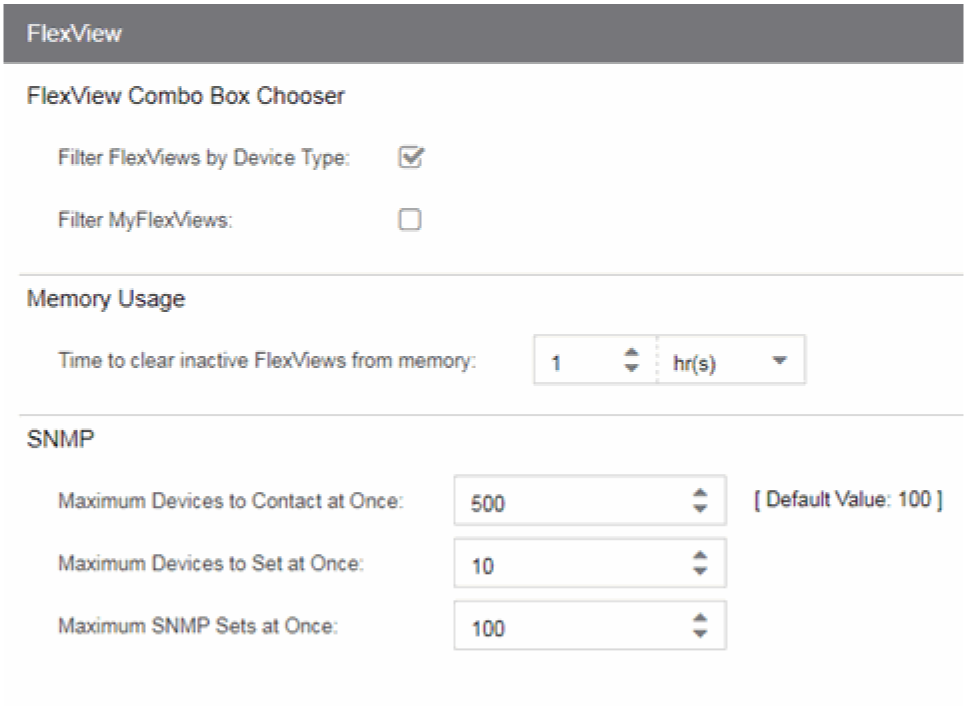
Update Credentials

Enter the credentials used to access the ExtremeNetworks.com website to obtain firmware and Extreme Management Center update information. You need to create an account at ExtremeNetworks.com and define a username and password for the account, then enter the same credentials here.

FlexView Options

Selecting FlexView in the left panel of the **Options** tab provides the following view, where you can configure the settings related to FlexViews in Extreme Management Center.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



FlexView

FlexView Combo Box Chooser

Filter FlexViews by Device Type: ☑

Filter MyFlexViews: □

Memory Usage

Time to clear inactive FlexViews from memory: 1 hr(s)

SNMP

Maximum Devices to Contact at Once: 500 [Default Value: 100]

Maximum Devices to Set at Once: 10

Maximum SNMP Sets at Once: 100

FlexView Combo Box Chooser

This section allows you to determine how FlexViews are displayed.

Filter FlexViews by Device Type

Select this box to filter FlexViews based on the device type.

Filter MyFlexViews

Select this checkbox to allow Extreme Management Center to filter FlexViews you create.

Memory Usage

Filter FlexViews by Device Type

The amount of time before Extreme Management Center removes inactive FlexViews from memory.

SNMP

These status polling options pertain to devices whose poll type is set to SNMP.

Maximum Devices to Contact at Once

The maximum number of IP addresses Extreme Management Center attempts to contact (read) simultaneously.

Maximum Devices to Set at Once

The maximum number of IP addresses Extreme Management Center attempts to perform PDU (protocol data unit) sets against simultaneously.

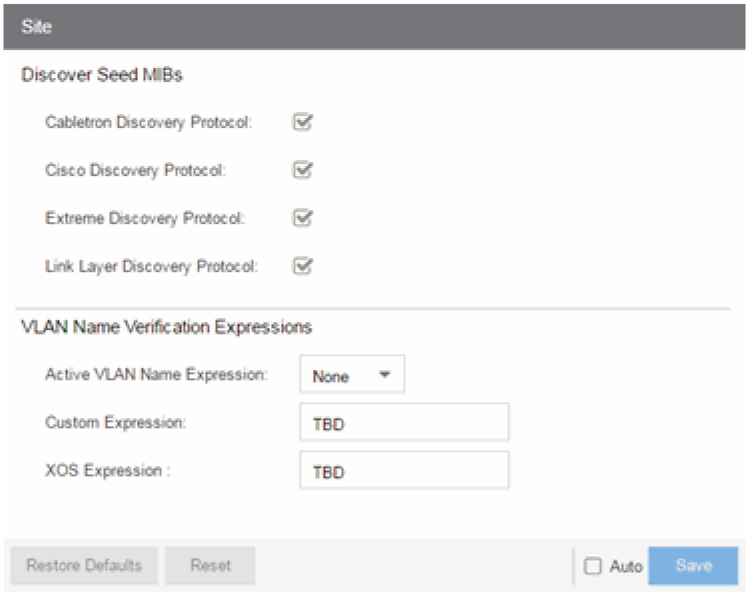
Maximum SNMP Sets at Once

The maximum number of SNMP PDU sets Extreme Management Center attempts to contact simultaneously.

Site Options

Selecting Site in the left panel of the **Options** tab provides the following view, where you can allow or deny specific protocols when discovering devices for a site.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Site

Discover Seed MIBs

Cabletron Discovery Protocol: ☑

Cisco Discovery Protocol: ☑

Extreme Discovery Protocol: ☑

Link Layer Discovery Protocol: ☑

VLAN Name Verification Expressions

Active VLAN Name Expression: None

Custom Expression: TBD

XOS Expression : TBD

Discovery Seed MIBs

Cabletron Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Cabletron Discovery Protocol (ctCDP) to detect devices to add to Extreme Management Center.

Cisco Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Cisco Discovery Protocol (CDP) to detect devices to add to Extreme Management Center.

Extreme Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Extreme Discovery Protocol (EDP) to detect devices to add to Extreme Management Center.

Link Layer Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Link Layer Discovery Protocol (LLDP) to detect devices to add to Extreme Management Center.

VLAN Name Verification Expressions

Active VLAN Name Expression

Select the set of rules Extreme Management Center uses to verify your operating system supports a VLAN Name.

Custom Expression

Enter a VLAN Name to verify your custom device's operating system supports a VLAN Name. The VLAN Name entered is verified against the rules selected in the Active VLAN Name Expression field.

XOS Expression

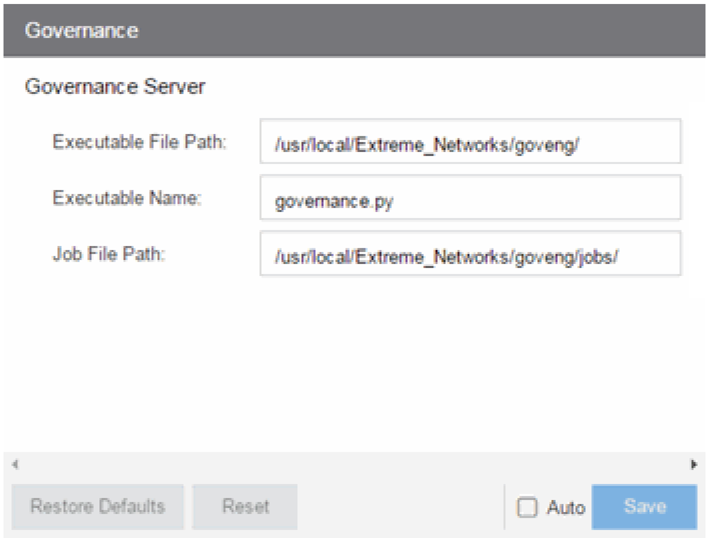
Enter a VLAN Name to verify your ExtremeXOS device's operating system supports a VLAN Name. The VLAN Name entered is verified against the rules selected in the Active VLAN Name Expression field.

Governance Options

The options on this tab are designed for functionality included in a future release.

Selecting Governance in the left panel of the **Options** tab provides the following view, where you can specify the Governance engine file name used by Extreme Management Center, the path to the directory in which the file is located, and the path to the job file directory. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Governance

Governance Server

Executable File Path: /usr/local/Extreme_Networks/goveng/

Executable Name: governance.py

Job File Path: /usr/local/Extreme_Networks/goveng/jobs/

Executable File Path

The directory in which the Governance engine executable file is located.

Executable Name

The name of the executable file used by the Governance engine.

Job File Path

The path to the directory in which the job files are located. The Governance engine uses job files to test device configurations in order to provide you with vulnerability information.

Impact Analysis Options

Selecting **Impact Analysis** in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the Impact Analysis dashboard. The right-panel view changes depending on what you select in the left-panel tree. Expand the Impact Analysis tree to view all the different available options. These settings apply to all users.

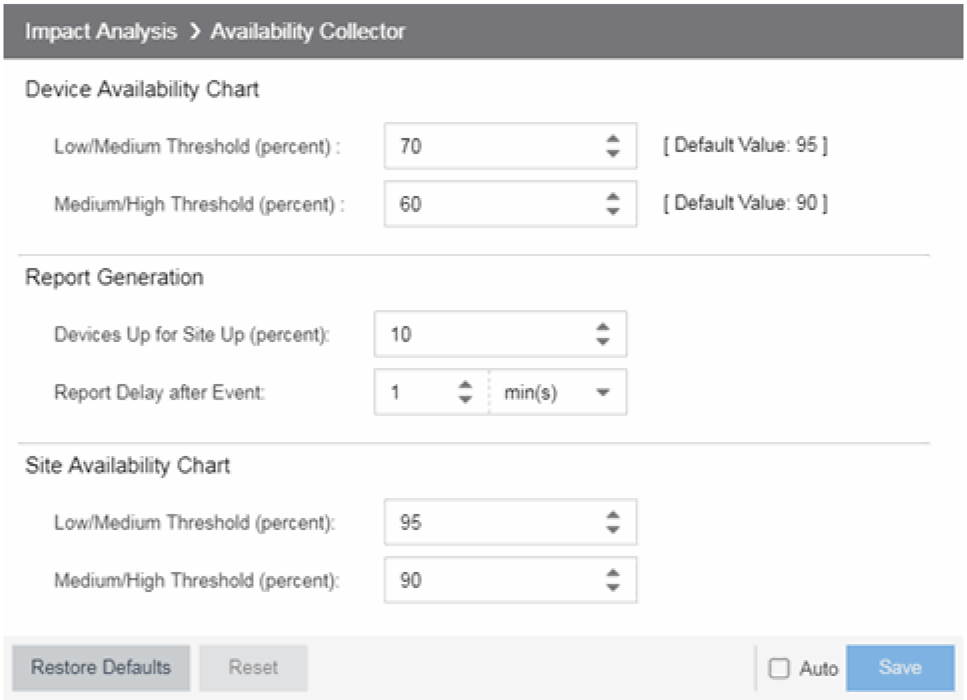
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Click the link for information on the following Impact Analysis options:

- Availability Collector
- Capacity/Health Collector
- Configuration Collector
- Performance Collector

Availability Collector

These options allow you to configure the threshold settings for the Site and Device Availability Charts in the Impact Analysis dashboard.



Impact Analysis > Availability Collector

Device Availability Chart

Low/Medium Threshold (percent) : 70 [Default Value: 95]

Medium/High Threshold (percent) : 60 [Default Value: 90]

Report Generation

Devices Up for Site Up (percent): 10

Report Delay after Event: 1 min(s)

Site Availability Chart

Low/Medium Threshold (percent): 95

Medium/High Threshold (percent): 90

Device Availability Chart

Low/Medium Threshold (percent)

Indicates the percentage of devices on your network that Extreme Management Center can reach. If the value falls below the percentage entered here, the Impact Status of the Device Availability chart moves from Low to Medium. For devices to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of devices on your network that Extreme Management Center can reach. If the value falls below the percentage entered here, the Impact Status of the Device Availability chart moves from Medium to High. For devices to be included, data collection must be enabled.

Report Generation

Devices Up for Site Up (percent)

Indicates the percent of devices included in a site that Extreme Management Center can reach. If the value falls below the percentage entered here, the Extreme Management Center considered the site down.

Report Delay after Event

Indicates the amount of time Extreme Management Center waits before reporting a device is down.

Site Availability Chart

Low/Medium Threshold (percent)

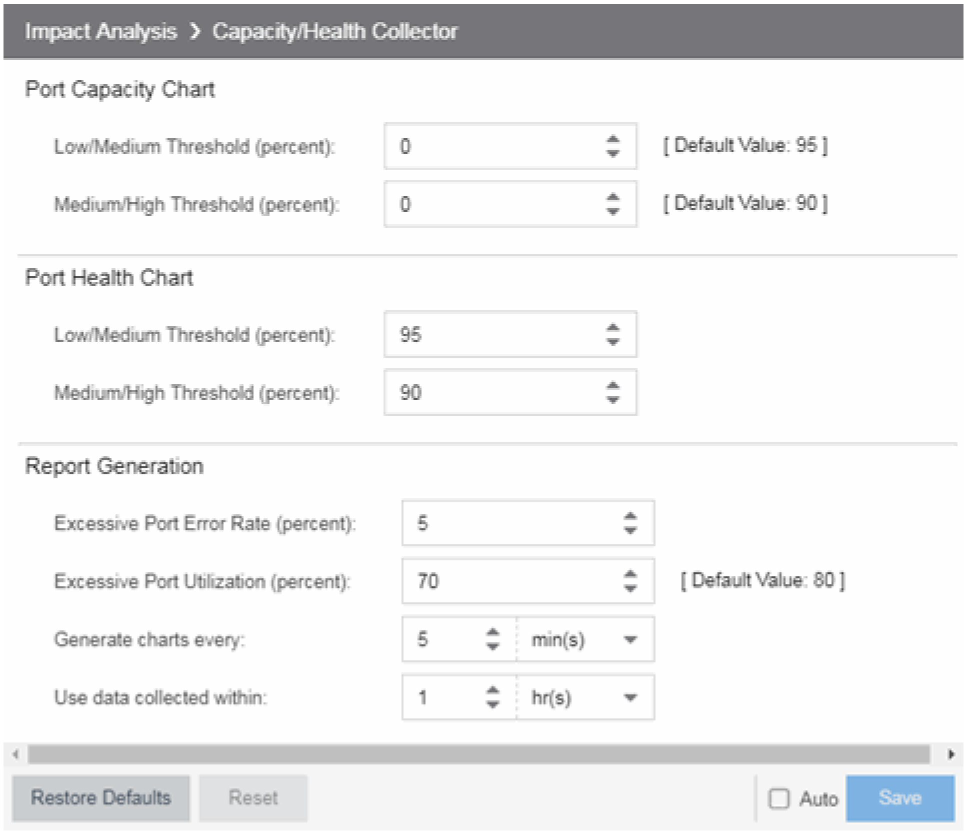
Indicates the percentage of devices included in a site that Extreme Management Center can reach. If the value falls below the percentage entered here, the **Impact Status** of the Site Availability chart moves from **Low** to **Medium**. For devices to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of devices included in a site that Extreme Management Center can reach. If the value falls below the percentage entered here, the **Impact Status** of the Site Availability chart moves from **Medium** to **High**. For devices to be included, data collection must be enabled.

Capacity/Health Collector

These options let you configure the thresholds for the Port Capacity and Port Health Charts in the Impact Analysis dashboard.



Impact Analysis > Capacity/Health Collector

Port Capacity Chart

Low/Medium Threshold (percent): 0 [Default Value: 95]

Medium/High Threshold (percent): 0 [Default Value: 90]

Port Health Chart

Low/Medium Threshold (percent): 95

Medium/High Threshold (percent): 90

Report Generation

Excessive Port Error Rate (percent): 5

Excessive Port Utilization (percent): 70 [Default Value: 80]

Generate charts every: 5 min(s)

Use data collected within: 1 hr(s)

Port Capacity Chart

Low/Medium Threshold (percent)

Indicates the percentage of ports on your network with an acceptable level of utilization. If the value falls below the percentage entered here, the **Impact Status** on the Port Capacity chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of ports on your network with an acceptable level of utilization. If the value falls below the percentage entered here, the **Impact Status** on the Port Capacity chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Port Health Chart

Low/Medium Threshold (percent)

Indicates the percentage of ports on your network with an acceptable error rate. If the value falls below the percentage entered here, the **Impact Status** on the Port

Health chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of ports on your network with an acceptable error rate. If the value falls below the percentage entered here, the **Impact Status** on the Port Health chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Report Generation

Excessive Port Error Rate (percent)

Indicates the port error rate, in percent of total port traffic, above which Extreme Management Center considers the port error rate excessive. A port error rate below this percentage is considered acceptable.

Excessive Port Utilization (percent)

Indicates the port utilization, in percent of total port traffic, above which Extreme Management Center considers the port utilization excessive. A port utilization below the percentage entered here is considered acceptable.

Generate charts every

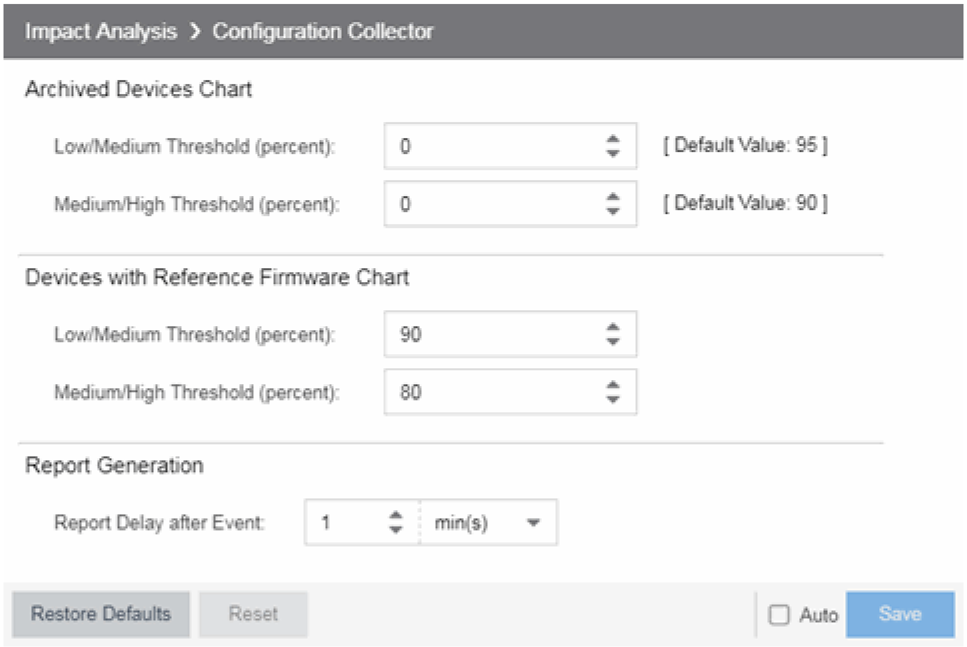
Indicates the interval between which Extreme Management Center polls ports to generate the Port Capacity and Port Health charts.

Use data collected within

Select the

Configuration Collector

These options allow you to configure the thresholds of the Archived Devices and the Devices with Reference Firmware charts in the Impact Analysis dashboard.



Impact Analysis > Configuration Collector

Archived Devices Chart

Low/Medium Threshold (percent): 0 [Default Value: 95]

Medium/High Threshold (percent): 0 [Default Value: 90]

Devices with Reference Firmware Chart

Low/Medium Threshold (percent): 90

Medium/High Threshold (percent): 80

Report Generation

Report Delay after Event: 1 min(s)

Archived Devices Chart

Low/Medium Threshold (percent)

Indicates the percentage of devices for which an archive was created in the last 30 days. If the value falls below the percentage entered here, the **Impact Status** on the Archived Devices chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of devices for which an archive was created in the last 30 days. If the value falls below the percentage entered here, the **Impact Status** on the Archived Devices chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Devices with Reference Firmware Chart

Low/Medium Threshold (percent)

Indicates the percentage of devices on which firmware you define as a reference image is installed. If the value falls below the percentage entered here, the **Impact Status** on the Devices with Reference Firmware chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of devices on which firmware you define as a reference image is installed. If the value falls below the percentage entered here, the **Impact Status** on the Devices with Reference Firmware chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Report Generation

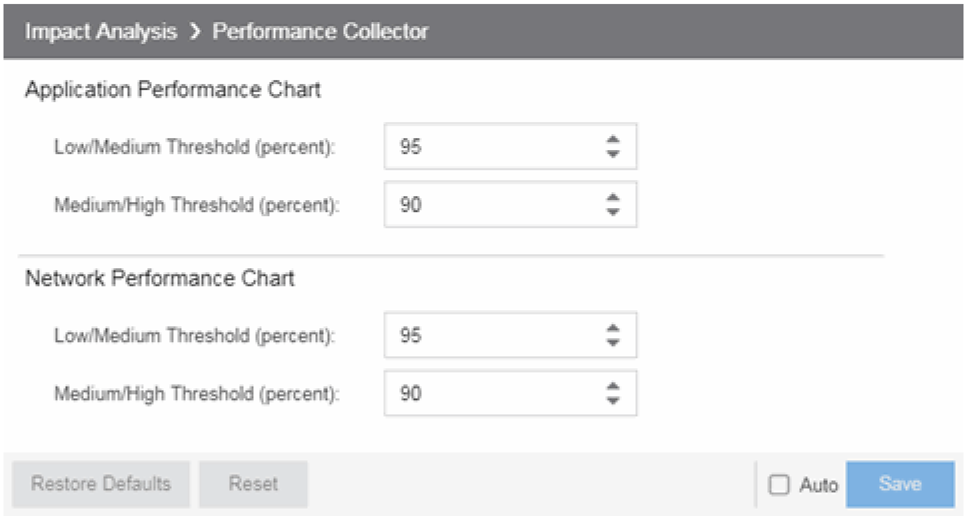
Report Delay after Event

Indicates the amount of time Extreme Management Center waits before reporting a device does not have an archive created in the last 30 days or does not have a reference firmware image installed.

Performance Collector

These options allow you to configure the thresholds of the Application and Network Performance charts in the Impact Analysis dashboard.

These options let you configure the amount of resources used by the end-system event cache.



Impact Analysis > Performance Collector

Application Performance Chart

Low/Medium Threshold (percent): 95

Medium/High Threshold (percent): 90

Network Performance Chart

Low/Medium Threshold (percent): 95

Medium/High Threshold (percent): 90

Application Performance Chart

Low/Medium Threshold (percent)

Indicates the percentage of tracked applications with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Application Performance chart moves from **Low** to **Medium**. The expected response time is established using an average of the previously observed response times, or using dynamic thresholding, if enabled.

Medium/High Threshold (percent)

Indicates the percentage of tracked applications with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Application Performance chart moves from **Medium** to **High**. The expected response time is established using an average of the previously observed response times, or using dynamic thresholding, if enabled.

Network Performance Chart

Low/Medium Threshold (percent)

Indicates the percentage of network services with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Network Performance chart moves from **Low** to **Medium**. The expected response time is established using an average of the previously observed response times, or using dynamic thresholding, if enabled.

Medium/High Threshold (percent)

Indicates the percentage of network services with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Network Performance chart moves from **Medium** to **High**. The expected response time is established using an average of the previously observed response times, or using dynamic thresholding, if enabled.

Related Information

For information on related topics:

- Impact Analysis Dashboard

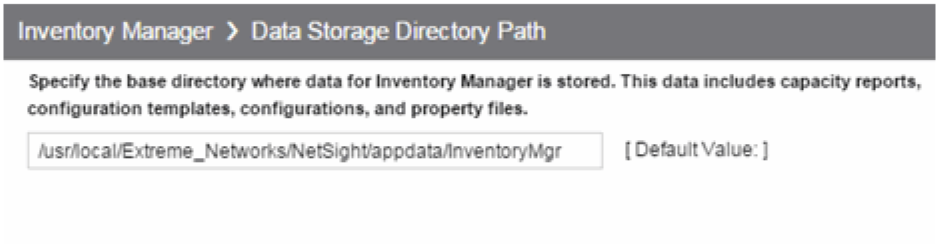
Inventory Manager Options

Selecting Inventory Manager in the left panel of the **Options** tab provides the following view, where you can select the path in which Inventory Manager data is stored as well as configure file transfer settings for firmware upgrades.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Data Storage Directory Path Setting

This option allows you to specify a different base directory where Inventory Manager data is stored. This data includes capacity planning reports, configuration templates, archived configurations, and property files. If you specify a new data directory, you need to move the data files stored under the old directory to the new directory so Extreme Management Center can find them.



Inventory Manager > Data Storage Directory Path

Specify the base directory where data for Inventory Manager is stored. This data includes capacity reports, configuration templates, configurations, and property files.

/usr/local/Extreme_Networks/NetSight/appdata/InventoryMgr [Default Value:]

File Transfer Settings

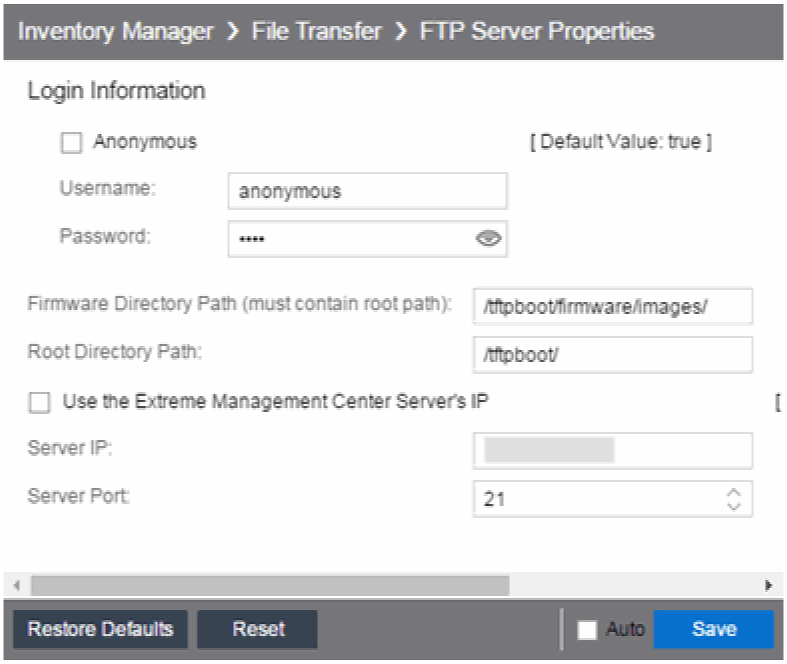
These options specify the FTP, SCP, or TFTP file transfer settings used when upgrading firmware.

Click the link for information on the following File Transfer Settings options:

- FTP Server Properties Settings
- SCP Server Properties Settings
- TFTP Server Properties Settings

FTP Server Properties Settings

These options allow you to set FTP server properties and login information. Use this view to specify the FTP server IP address, set paths to the root and firmware directories, and set login information. The FTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.



Inventory Manager > File Transfer > FTP Server Properties

Login Information

□ Anonymous [Default Value: true]

Username: anonymous

Password: ••••

Firmware Directory Path (must contain root path): /tftpboot/firmware/images/

Root Directory Path: /tftpboot/

□ Use the Extreme Management Center Server's IP

Server IP:

Server Port: 21

Anonymous

Select this checkbox if your FTP server is configured to accept Anonymous logins. Selecting this checkbox disables the **Username** and **Password** fields.

Username/Password

Enter your username and password to access the FTP server. By default, your password is displayed as a series of asterisks. Select the **Eye** icon to display your password.

Firmware Directory Path

The default firmware directory is tftpboot\firmware\images. If you would like to use an alternate firmware directory, enter a path to that directory in this field. The firmware directory must be a subdirectory of the root directory. (For additional information, see How to Upgrade Firmware.) If you are using an FTP server on a remote system, use the UNC standard described in the following Note when specifying the path.

Root Directory Path

The root directory is the base directory to which the FTP server is allowed access. The FTP server is allowed to create files in or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory Extreme Management Center automatically creates when it is installed. To use an alternate root directory, enter a path to that directory in this field.

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your FTP server is configured with an FTP root directory, it must match the root directory entered here.
- If your FTP server is **not** configured with an FTP root directory, change the FTP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
- **If you are using an FTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the tftpboot directory on the remote drive)
  use
  `\\yourservername\tftpboot\`

Use the Extreme Management Center Server's IP

Select this checkbox if your FTP server is on the same machine as the Extreme Management Center Server. Selecting this checkbox disables the **Server IP** field.

Server IP

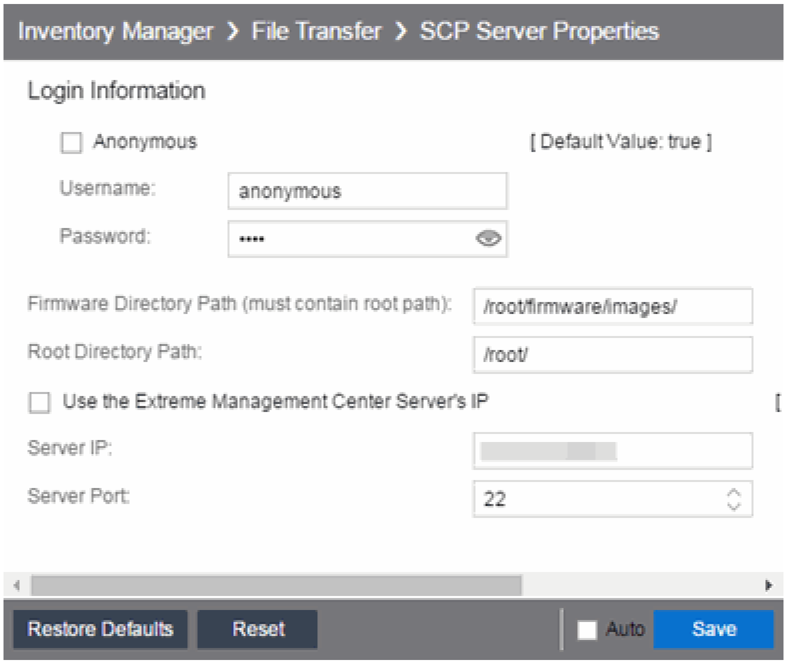
Enter the IP address of the device where the FTP server resides.

Server Port

Specify the port number on which your FTP server is configured to run.

SCP Server Properties Settings

These options allow you to set SCP server properties and login information. Use this view to specify the SCP server IP address, set paths to the root and firmware directories, and set login information. The SCP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.



Inventory Manager > File Transfer > SCP Server Properties

Login Information

□ Anonymous [Default Value: true]

Username: anonymous

Password: ••••

Firmware Directory Path (must contain root path): /root/firmware/images/

Root Directory Path: /root/

□ Use the Extreme Management Center Server's IP [

Server IP: [redacted]

Server Port: 22

Anonymous

Select this checkbox if your SCP server is configured to accept Anonymous logins. Selecting this checkbox disables the **Username** and **Password** fields.

Username/Password

Enter your username and password to access the SCP server. By default, your password is displayed as a series of asterisks. Select the **Eye** icon to display your password.

Firmware Directory Path

Enter the path to the default firmware directory in this field. The **Firmware Directory Path** must be a subdirectory of the Root Directory Path. On a Linux system, the default firmware directory is `/root/firmware/images/`. On a Windows system, an SCP server is not installed by default, so the default **Firmware Directory Path** is `C:\tftpboot\firmware\images\`. This path needs to be updated once the

SCP server is installed and a valid directory is created. For additional information, see How to Upgrade Firmware. If you are using an SCP server on a remote system, use the UNC standard described in the following Note when specifying the path.

Root Directory Path

Enter the path to the root directory in this field. The root directory is the base directory to which the SCP server is allowed access. The SCP server is allowed to create files in or read files from this directory and any of its subdirectories. On a Linux system, the default root directory is `/root/`. On a Windows system, an SCP server is not installed by default, so the default **Root Directory Path** is `C:\tftpboot\`. This path needs to be updated once the SCP server is installed and a valid directory is created.

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your SCP server is configured with an SCP root directory, it must match the root directory entered here.
- If your SCP server is **not** configured with an SCP root directory, change the SCP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
- **If you are using an SCP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the firmware\images directory on the remote drive)
  use
  `\\yourservername\firmware\images`

Use the Extreme Management Center Server's IP

Select this checkbox if your SCP server is on the same machine as the Extreme Management Center Server. Selecting this checkbox disables the **Server IP** field.

Server IP

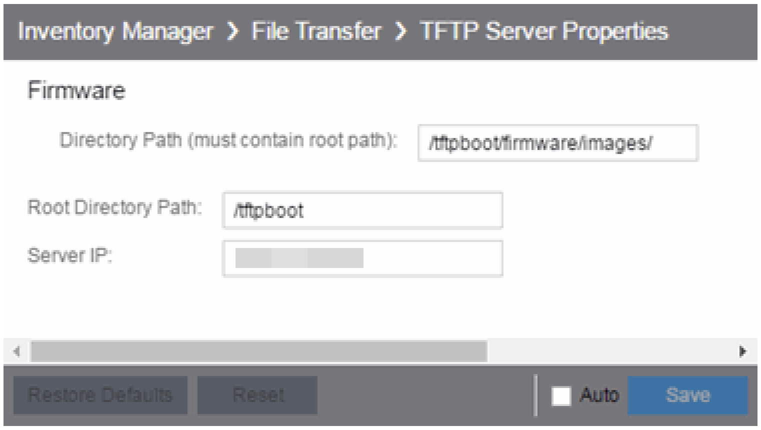
Enter the IP address of the device where the SCP server resides.

Server Port

Specify the port number on which your SCP server is configured to run.

TFTP Server Properties Settings

These options allow you to set TFTP server properties. This view lets you set the firmware directory path, the TFTP root directory path, and server IP address. These settings apply to all users.



Firmware

Directory Path (must contain root path): /tftpboot/firmware/images/

Root Directory Path: /tftpboot

Server IP: [redacted]

Directory Path

The default firmware directory is `tftpboot\firmware\images`. If you would like to use an alternate firmware directory, enter a path to that directory in this field. The firmware directory must be a subdirectory of the root directory. (For additional information, see How to Upgrade Firmware.)

Root Directory Path

The root directory is the base directory to which the TFTP server is allowed access. The TFTP server is allowed to create files in or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory Extreme Management Center automatically creates when it is installed. To use an alternate root directory, enter a path to that directory in this field.

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.
- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive (e.g. C:\ for Windows and /root/ for Linux).
- **If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the firmware\images directory on the remote drive)
  use
  `\\yourservername\firmware\images`

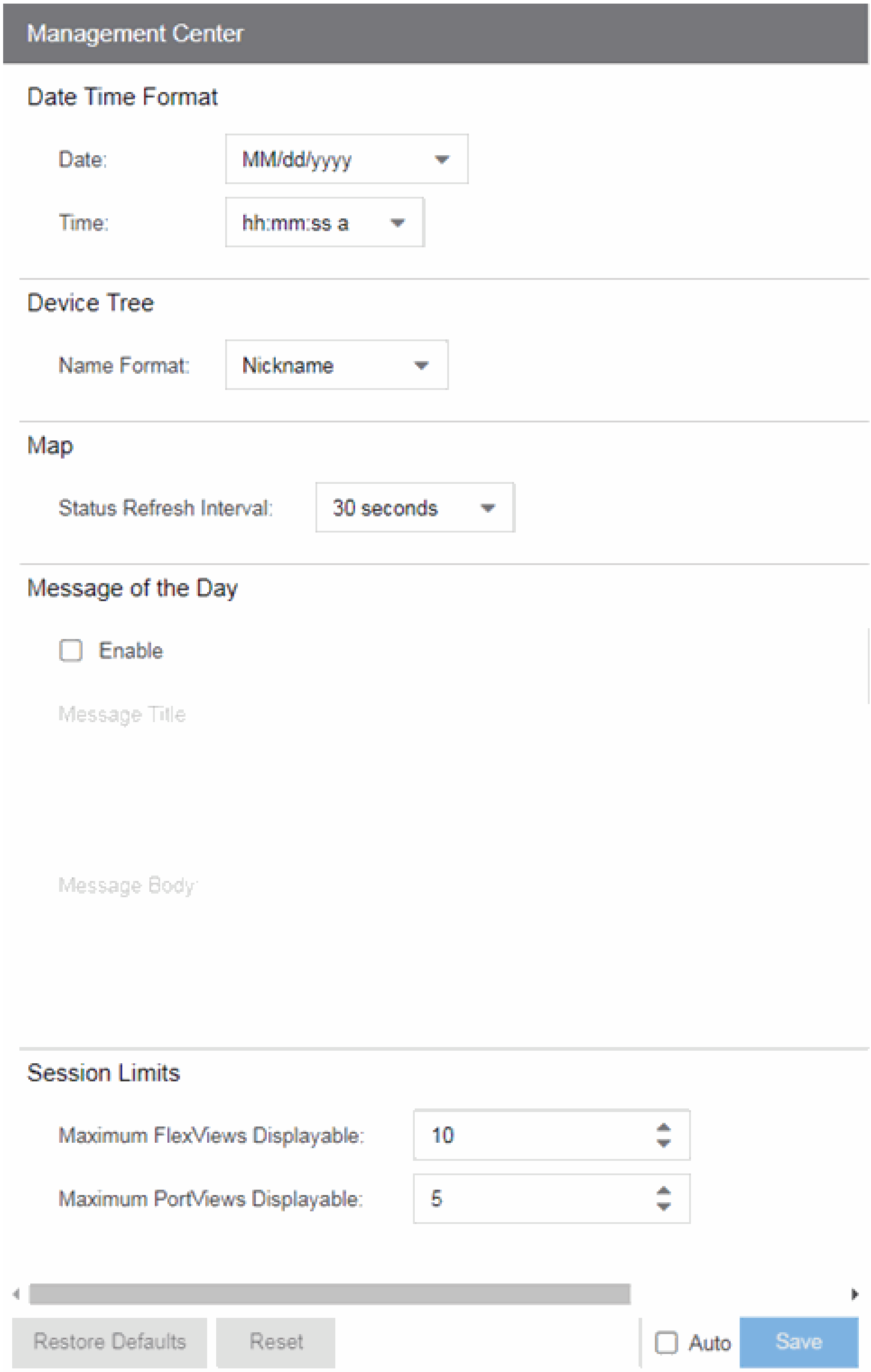
Server IP

Enter the IP address of the device where the TFTP server resides.

Options

Selecting Extreme Management Center in the left panel of the **Options** tab provides the following view, where you can customize Extreme Management Center preferences. These settings apply to the user currently logged-in.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Management Center

Date Time Format

Date: MM/dd/yyyy

Time: hh:mm:ss a

Device Tree

Name Format: Nickname

Map

Status Refresh Interval: 30 seconds

Message of the Day

☐ Enable

Message Title

Message Body:

Session Limits

Maximum FlexViews Displayable: 10

Maximum PortViews Displayable: 5

Date Time Format

Date

Select how the date is formatted in Extreme Management Center.

The letters in this field signify the following:

- MM — Month
- dd — Day
- yyyy — Year

Time

Select whether time is formatted as a 12-hour (hh:mm:ss a) or 24-hour (HH:mm:ss) clock.

The letters in this field signify the following:

- hh — Hour
- mm — Minute
- ss — Second

Device Tree

Name Format

Select one of the following options:

- IP — use the device's IP address.
- System Name — use the administratively-assigned name of the device taken from the *sysName* MIB object.
- Nickname — use the user-defined nickname as defined in the Edit Devices window.

Map

Status Refresh Interval

Select the interval that determines how often maps are automatically refreshed by Extreme Management Center. If None is selected, maps must be manually refreshed.

Message of the Day

Enable

Select the checkbox to enable the **Message Title** and **Message Body** fields, where you can enter a message that displays to all users accessing Extreme Management Center.

Message Title

Enter a title for the message displayed to all Extreme Management Center users when the **Enable** checkbox is selected.

Message Body

Enter a body for the message displayed to all Extreme Management Center users when the **Enable** checkbox is selected.

Session Limits

Maximum FlexViews Displayable

Allows you to determine the maximum number of FlexViews displayed per session.

Maximum PortViews Displayable

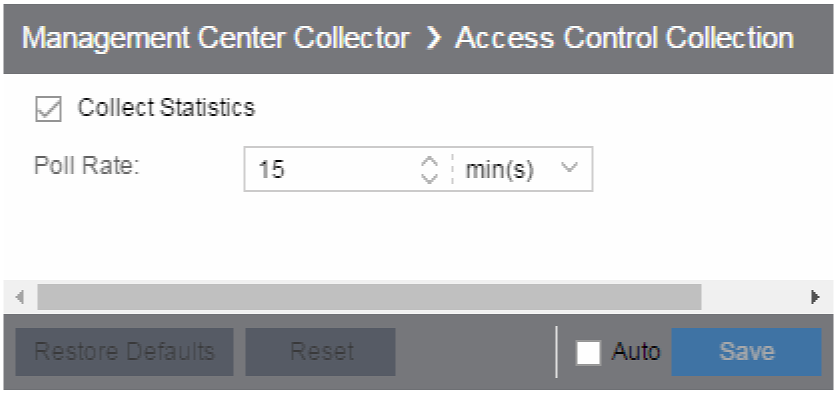
Allows you to determine the maximum number of PortViews displayed per session.

Collector Options

Selecting Extreme Management Center Collector in the left panel of the **Options** tab provides the following view, where you can configure Extreme Management Center Collector tree settings. These settings let you access advanced device and interface collection settings for the Extreme Management Center Collector.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Access Control Collection



Management Center Collector > Access Control Collection

☑ Collect Statistics

Poll Rate: 15 min(s)

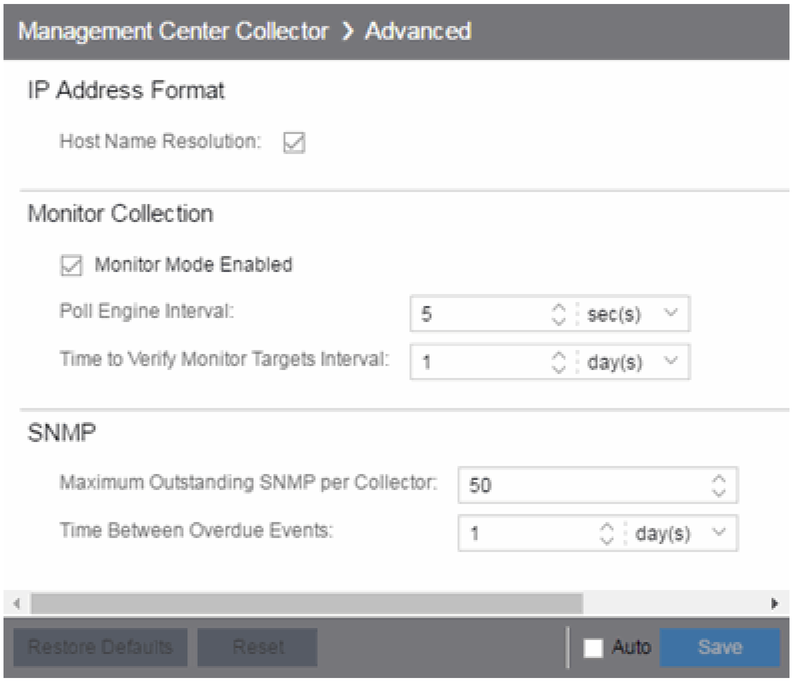
Collect Statistics

Select this checkbox to enable Extreme Access Control data collection.

Poll Rate

The amount of time the data collector waits between polling Extreme Access Control engines.

Advanced



Management Center Collector > Advanced

IP Address Format

Host Name Resolution: ☑

Monitor Collection

☑ Monitor Mode Enabled

Poll Engine Interval: 5 sec(s)

Time to Verify Monitor Targets Interval: 1 day(s)

SNMP

Maximum Outstanding SNMP per Collector: 50

Time Between Overdue Events: 1 day(s)

Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for this feature only. (Host name resolution is enabled globally using the Enable Name Resolution option.)

Monitor Mode Enabled

Use this option to enable or disable monitor mode statistic collection. If monitor mode is disabled, the **Monitor Mode** option is not available when configuring device or interface statistics collection. All monitor mode statistic collection is stopped and the monitor cache is cleared. For additional information, see Enable Report Data Collection.

Poll Engine Interval

This interval specifies the frequency the data collector polls the collection targets. Polling is performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Time to Verify Monitor Targets Interval

The interval between a check of all targets (devices and interfaces) set to Monitor mode statistic collection. The check generates a summary event in the **Alarms and**

Events tab event log (one for devices and one for interfaces) that shows the number of targets where corresponding threshold alarms are not configured. Disable Monitor mode for those targets or configure appropriate threshold alarms in order to reduce unnecessary statistic collection.

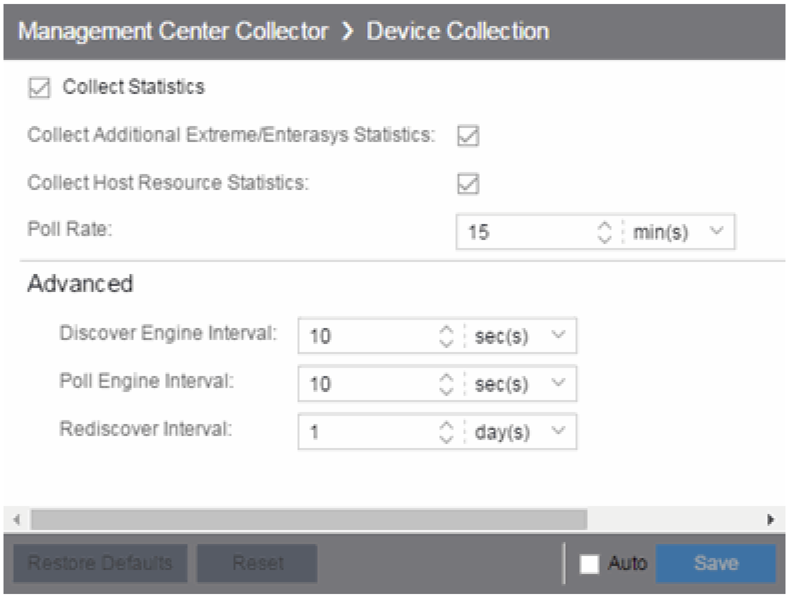
Maximum Outstanding SNMP per Collector

The number of simultaneous SNMP requests a collector can make. The data collector works with blocks of SNMP requests, starting a new block each time the outstanding block completes. Valid values are 1-500.

Time Between Overdue Events

During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

Device Collection



Management Center Collector > Device Collection

☑ Collect Statistics

Collect Additional Extreme/Enterasys Statistics: ☑

Collect Host Resource Statistics: ☑

Poll Rate: 15 min(s)

Advanced

Discover Engine Interval: 10 sec(s)

Poll Engine Interval: 10 sec(s)

Rediscover Interval: 1 day(s)

Collect Statistics

Enables or disables additional statistics collection.

Collect Additional Extreme/Enterasys Statistics

Enables or disables Extreme and Enterasys switch resource statistics collection.

Collect Host Resource Statistics

Enables or disables host resource statistics collection.

Poll Rate

The amount of time the data collector waits between polling devices.

Discover Engine Interval

This interval specifies the frequency with which the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

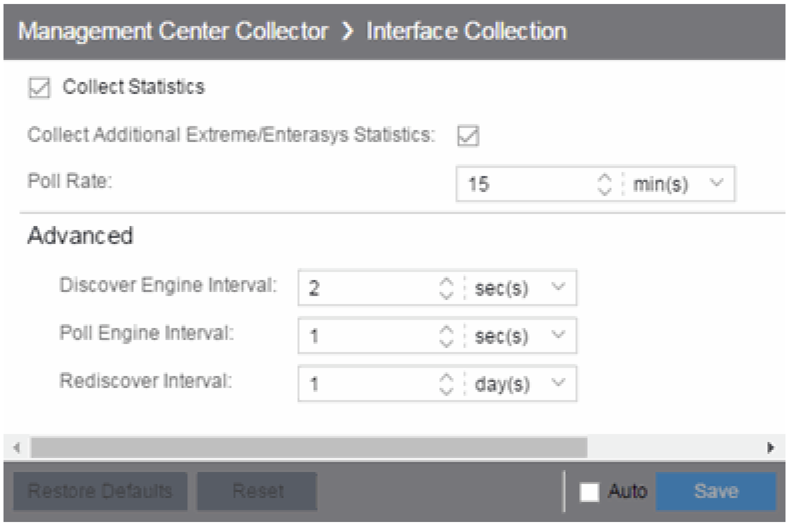
Poll Engine Interval

This interval specifies the frequency with which the data collector polls the collection targets. Polling is performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

Rediscover Interval

This interval specifies the frequency with which the data collector performs a rediscover operation on the collection targets.

Interface Collection



Management Center Collector > Interface Collection

☑ Collect Statistics

Collect Additional Extreme/Enterasys Statistics: ☑

Poll Rate: 15 min(s)

Advanced

Discover Engine Interval: 2 sec(s)

Poll Engine Interval: 1 sec(s)

Rediscover Interval: 1 day(s)

Collect Statistics

Enables or disables additional statistics collection.

Collect Additional Extreme/Enterasys Statistics

Enables or disables Extreme and Enterasys switch resource statistics collection.

Poll Rate

The amount of time the data collector waits between polling devices.

Discover Engine Interval

This interval specifies the frequency with which the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

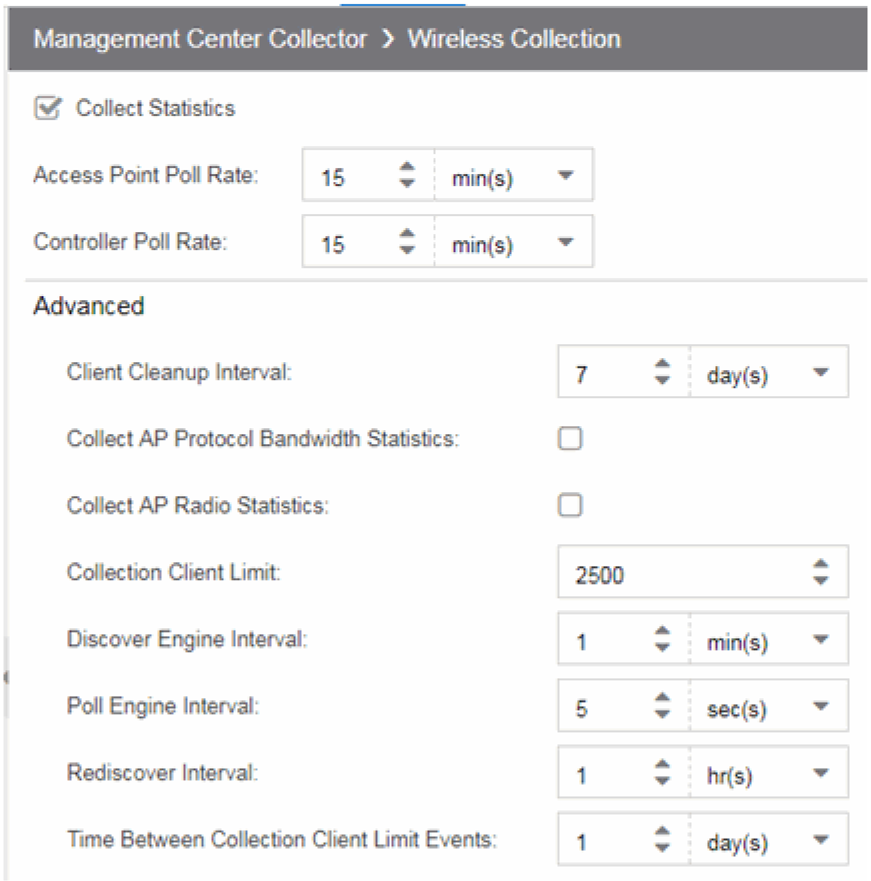
Poll Engine Interval

This interval specifies the frequency with which the data collector polls the collection targets. Polling is performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

Rediscover Interval

This interval specifies the frequency with which the data collector performs a rediscover operation on the collection targets.

Wireless Collection



Management Center Collector > Wireless Collection

☑ Collect Statistics

Access Point Poll Rate: 15 min(s)

Controller Poll Rate: 15 min(s)

Advanced

Client Cleanup Interval: 7 day(s)

Collect AP Protocol Bandwidth Statistics: □

Collect AP Radio Statistics: □

Collection Client Limit: 2500

Discover Engine Interval: 1 min(s)

Poll Engine Interval: 5 sec(s)

Rediscover Interval: 1 hr(s)

Time Between Collection Client Limit Events: 1 day(s)

Collect Statistics

Use this checkbox to enable or disable wireless data collection.

Access Point Poll Rate

The amount of time the data collector waits between polling wireless access points. Valid values are 1-60 minutes.

Controller Poll Rate

The amount of time the data collector waits between polling wireless controllers. Valid values are 1-60 minutes.

Client Cleanup Interval

Wireless client statistics stored by the data collector are periodically cleaned up according to this interval. When the Collection Client Limit is reached, clients inactive longer than the time specified in the Time Between Collection Client Limit Events are aged out.

Collect AP Protocol Bandwidth Statistics

Select the checkbox to collect protocol bandwidth statistics for your access points.

NOTE: The statistics collected in this report are used in the Venue Report. Only enable this option if you use that report.

Collect AP Protocol Radio Statistics

Select the checkbox to collect radio statistics for your access points.

NOTE: The statistics collected in this report are used in the Venue Report. Only enable this option if you use that report.

Collection Client Limit

The maximum number of wireless clients for which statistics are stored per collection interval. Valid values are 1 to 30,000.

Discover Engine Interval

This interval specifies the frequency the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

Poll Engine Interval

This interval specifies the frequency with which the data collector polls the collection targets. Polling is performed in blocks specified by the Maximum Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here.

Rediscover Interval

This interval specifies the frequency the data collector performs a rediscover operation on the collection targets.

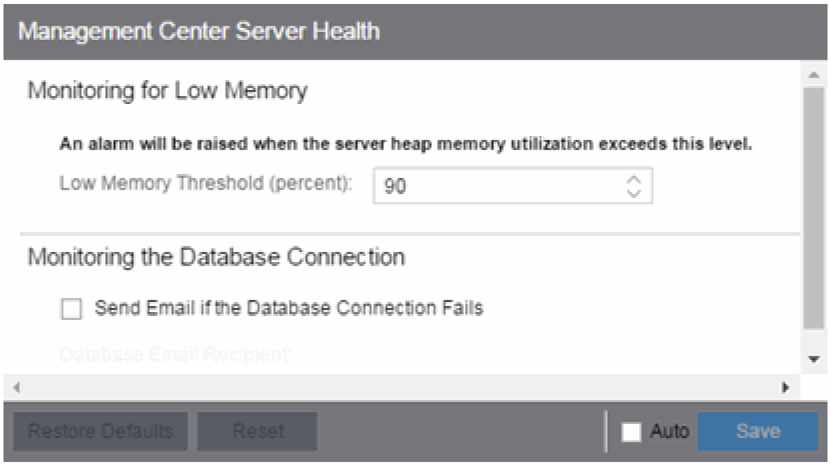
Time Between Collection Client Limit Events

During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

Server Health Options

Selecting Extreme Management Center Server Health in the left panel of the Options tab provides the following view, where you can configure warnings to help monitor the Extreme Management Center server health.

Changing a value from the system default causes a Default Value button to appear. Clicking this button changes the field back to the system default value.



Management Center Server Health

Monitoring for Low Memory

An alarm will be raised when the server heap memory utilization exceeds this level.

Low Memory Threshold (percent): 90

Monitoring the Database Connection

□ Send Email if the Database Connection Fails

Database Email Recipient

Monitoring for Low Memory

Low Memory Threshold (percent)

Enter a percentage to specify the server heap memory utilization percentage above which an alarm is raised. If the memory utilization falls more than five percent below the threshold percentage, the alarm is automatically cleared.

Monitoring the Database Connection

Send Email if the Database Connection Fails

Select the checkbox to send an email notification if the Extreme Management Center database goes down, and when the database comes back up again.

Database Email Recipient

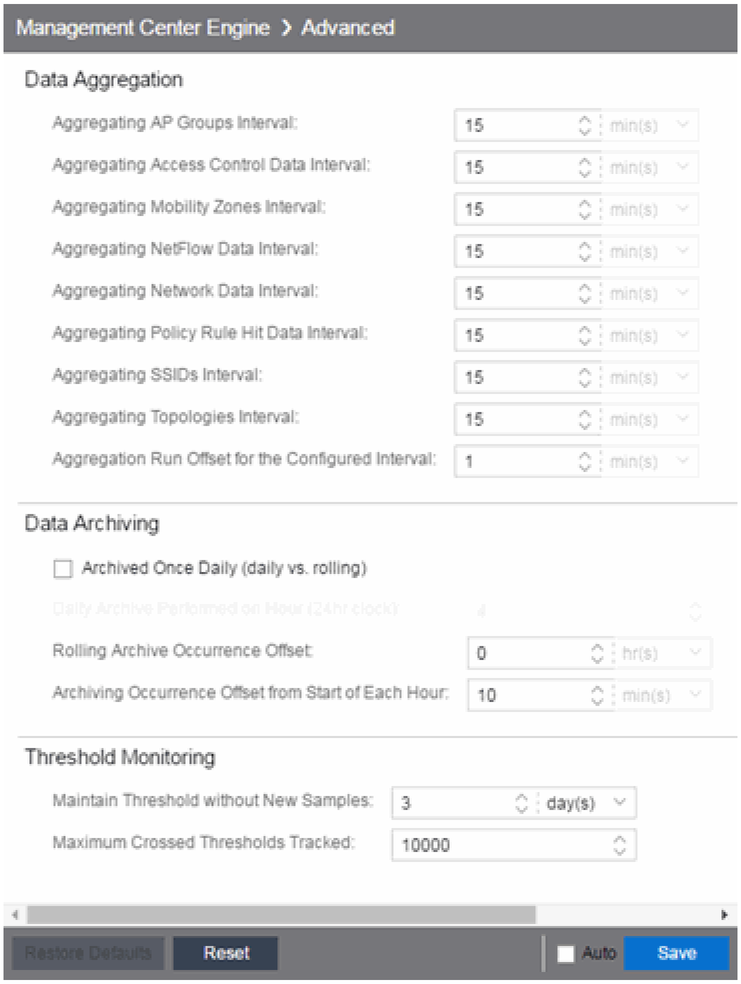
If Send Email if the Database Connection Fails is selected, enter the email address of the person to whom the email notification is sent.

Engine Options

Selecting Extreme Management Center Engine in the left panel of the **Options** tab provides the following view, where you can specify data aging options and advanced settings for data archiving and aggregation.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Advanced



Data Aggregation

Aggregating AP Groups Interval: 15 min(s)

Aggregating Access Control Data Interval: 15 min(s)

Aggregating Mobility Zones Interval: 15 min(s)

Aggregating NetFlow Data Interval: 15 min(s)

Aggregating Network Data Interval: 15 min(s)

Aggregating Policy Rule Hit Data Interval: 15 min(s)

Aggregating SSIDs Interval: 15 min(s)

Aggregating Topologies Interval: 15 min(s)

Aggregation Run Offset for the Configured Interval: 1 min(s)

Data Archiving

☐ Archived Once Daily (daily vs. rolling)

Daily Archive Performed on Hour (24hr clock): 4

Rolling Archive Occurrence Offset: 0 hr(s)

Archiving Occurrence Offset from Start of Each Hour: 10 min(s)

Threshold Monitoring

Maintain Threshold without New Samples: 3 day(s)

Maximum Crossed Thresholds Tracked: 10000

Data Aggregation

Use the data aggregation settings to specify how often collected data is aggregated into one statistic for AP Groups, Mobility Zones, SSIDs, Topologies, Policy Rule Hits, Network, Extreme Access Control, and NetFlow. For example, the data collected for all the APs in an AP group are aggregated into one AP Group statistic according to the specified interval. Intervals are based on the 0 minute of the hour, so with an interval of 15 minutes, the aggregation is performed every 15 minutes starting from the top of the hour. The offset allows for the time it takes for data to be collected and reported to the database. If the offset is too short, then the aggregation may be performed before all the data is reported to the database. In the case where there is a long latency in reporting data to the database, increase the offset in order to make sure all the data is included in the aggregation.

Data Archiving

Use the data archiving settings to specify whether collection data should be archived on a daily basis or rolling basis (the default).

- Daily Archive — Select this checkbox to archive all the collection data (including the raw data, and the hourly, daily, weekly, and monthly data) once a day at a certain time. The Daily Archive Performed on Hour (24) field displays, where you can specify the hour of day to perform the daily archive. The number entered in this field represents the time, so a value of 0 signifies midnight, while a value of 20 signifies 8:00 PM.
- Rolling Archive — If you want the collection data to be archived on a rolling basis (archives are performed on an hourly, daily, weekly, or monthly basis as needed), specify the offset (in hours and minutes) the rolling archive is performed, following the end of the data collection period. The offset allows for the time it takes for data to be collected and reported to the database. If the offset time is too short, then the archive may be performed before all the data is reported to the database. In cases with a long latency in reporting data to the database, you may need to increase the offset in order to make sure all the data is included in the archive.

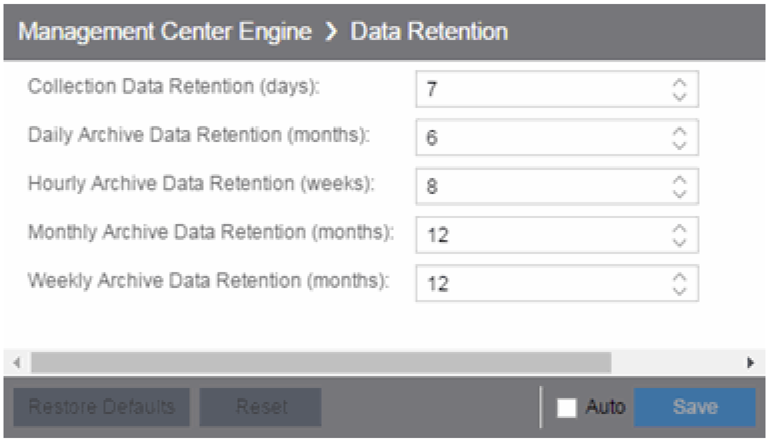
Threshold Monitoring

These settings apply to threshold alarms:

- Maintain Threshold without New Samples — Determines when a crossed threshold state expires due to inactivity (no new samples received). The default length of time is 72 hours. If there are no samples received during this time period, the threshold state is deleted and the associated alarm is cleared.

- **Maximum Crossed Thresholds Tracked** — To prevent memory over-utilization, there is a maximum number of crossed threshold states that are maintained. The default maximum number is 10,000. If this number is exceeded, the oldest 10% are deleted and the associated alarm is cleared.

Data Retention



Management Center Engine > Data Retention

Collection Data Retention (days): 7

Daily Archive Data Retention (months): 6

Hourly Archive Data Retention (weeks): 8

Monthly Archive Data Retention (months): 12

Weekly Archive Data Retention (months): 12

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)

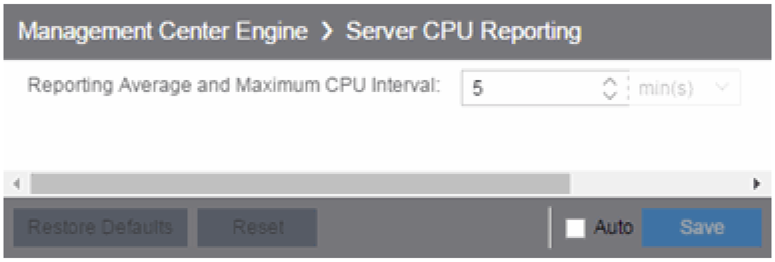
Every month, the weekly data is condensed into monthly average values and archived. This setting specifies how long (in months) to maintain the archived monthly data. Valid values are 1-200 months.

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



Management Center Engine > Server CPU Reporting

Reporting Average and Maximum CPU Interval: 5 min(s)

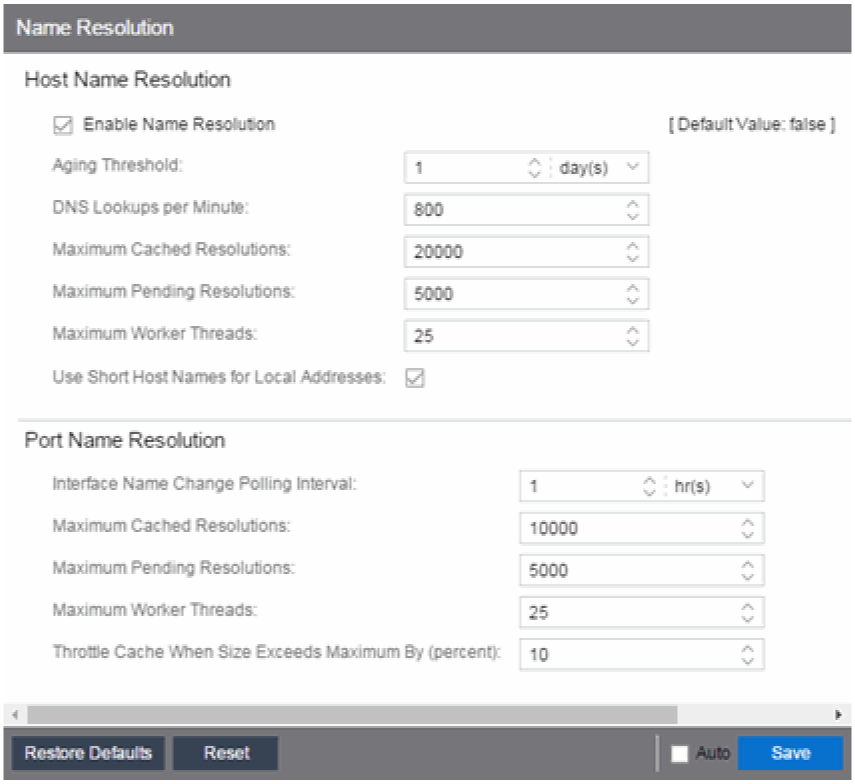
Reporting Average and Maximum CPU Interval

Extreme Management Center collects CPU usage statistics monitoring for the Extreme Management Center server. At 5 minute intervals (the default interval) the collected usage data is averaged, and the average and maximum statistics are reported to the Extreme Management Center database to provide data for the Extreme Management Center Server CPU Utilization report. You can change the default interval setting here, if desired. A shorter interval provides a more granular picture of CPU usage while a longer interval would mean that less data is stored in the database. Valid values are 1-59 minutes.

Name Resolution Options

Selecting Name Resolution in the left panel of the **Options** tab displays the following view, where you can configure options related to host name and port name resolution.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Name Resolution

Host Name Resolution

☑ Enable Name Resolution [Default Value: false]

Aging Threshold: 1 day(s)

DNS Lookups per Minute: 800

Maximum Cached Resolutions: 20000

Maximum Pending Resolutions: 5000

Maximum Worker Threads: 25

Use Short Host Names for Local Addresses: ☑

Port Name Resolution

Interface Name Change Polling Interval: 1 hr(s)

Maximum Cached Resolutions: 10000

Maximum Pending Resolutions: 5000

Maximum Worker Threads: 25

Throttle Cache When Size Exceeds Maximum By (percent): 10

□ Auto

Host Name Resolution

Use this section to set options for resolving host names to IP addresses and IP addresses to host names.

Enable Name Resolution

This option allows host names to be displayed in place of IP addresses throughout Extreme Management Center. This feature is primarily used by NetFlow. With name resolution enabled, flow data would show "Client=rsmith-ws Server=proxy-usa", rather than "client=10.20.0.2 server = 10.20.0.1". The option is off by default because name resolution can add additional load on the network's DNS server.

Aging Threshold

This option determines how long IP/host name pairs are cached in memory. After the aging threshold time has passed, the IP/host name pair is removed from the cache in order to prevent stale IP/host name associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, host names continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

DNS Lookups per Minute

The maximum number of host name lookups that the DNS server can perform each minute. This prevents host name resolution from using so many resources on a switch, which may affect switching of real traffic.

Maximum Cached Resolutions

The maximum number of IP/host name pairs that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum Pending Resolutions

The maximum number of host name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Maximum Worker Threads

The maximum number of host name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by host name resolution.

Use Short Host Names for Local Addresses

This option is enabled by default when host name resolution is enabled. When enabled, the host name cache removes the fully qualified host name's domain if it matches one of the specified local address domains. For example, "jsmith-ws.mycompany.com" would display as "jsmith-ws" if mycompany.com is listed as a local address domain. This option can be disabled when troubleshooting problems with host name resolution, or if IP addresses are preferred.

Port Name Resolution

Use this section to set options for resolving device port indices to port names and port aliases, and device port names and port aliases to port indices.

Interface Name Change Polling Interval

This option specifies how often the port name resolution service checks devices to see if port information has changed.

Maximum Cached Resolutions

The maximum amount of port data that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum Pending Resolutions

The maximum number of port name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Maximum Worker Threads

The maximum number of port name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by port name resolution.

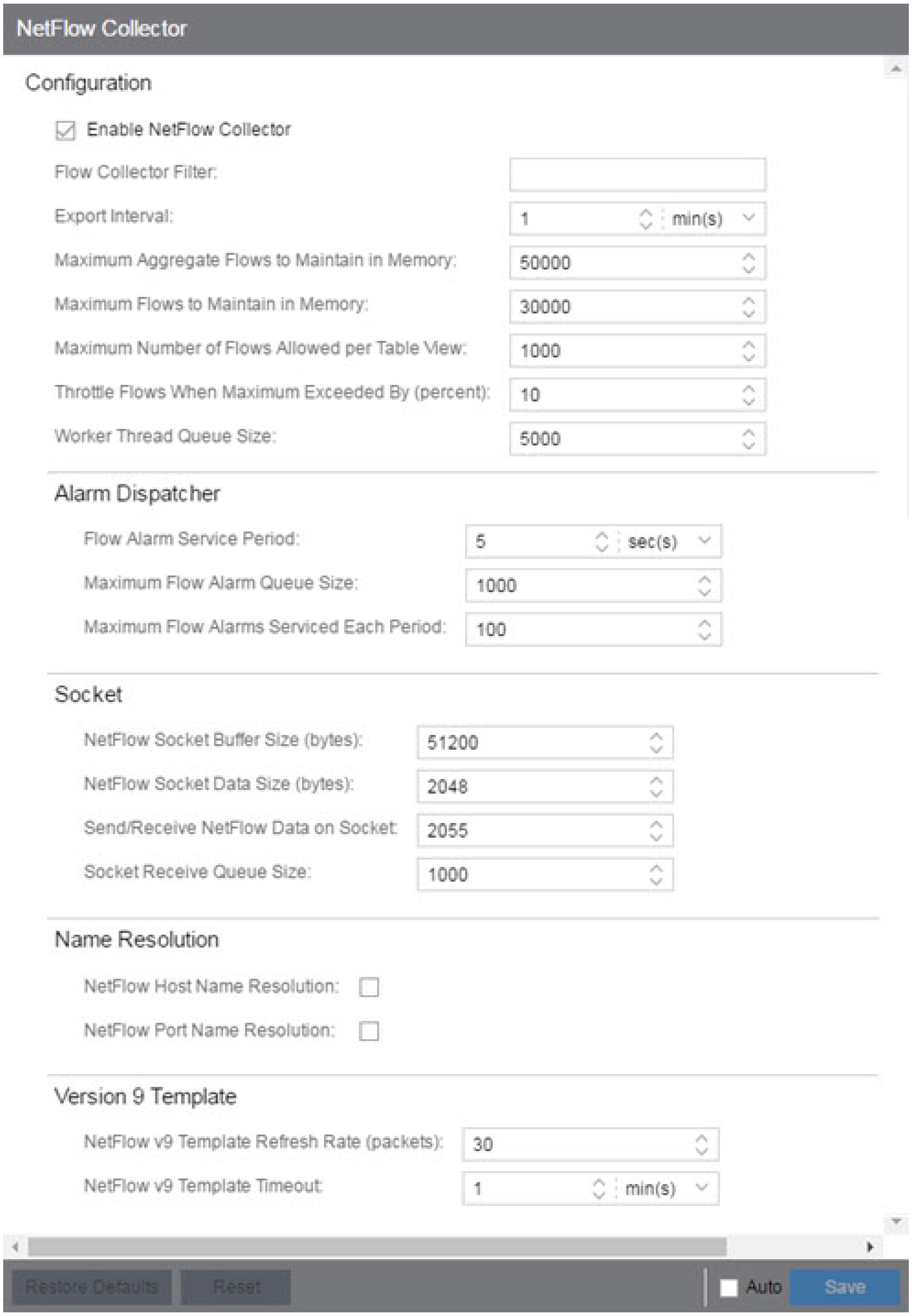
Throttle Cache When Size Exceeds Maximum By (percent)

This option controls how much port data is discarded from the cache when its size is exceeded. Adjust this to control how an overfull cache is reduced.

NetFlow Collector Options

Selecting NetFlow Collector in the left panel of the **Options** tab provides the following view, where you can configure NetFlow Collector settings in Extreme Management Center.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



NetFlow Collector

Configuration

☑ Enable NetFlow Collector

Flow Collector Filter:

Export Interval: 1 min(s)

Maximum Aggregate Flows to Maintain in Memory: 50000

Maximum Flows to Maintain in Memory: 30000

Maximum Number of Flows Allowed per Table View: 1000

Throttle Flows When Maximum Exceeded By (percent): 10

Worker Thread Queue Size: 5000

Alarm Dispatcher

Flow Alarm Service Period: 5 sec(s)

Maximum Flow Alarm Queue Size: 1000

Maximum Flow Alarms Serviced Each Period: 100

Socket

NetFlow Socket Buffer Size (bytes): 51200

NetFlow Socket Data Size (bytes): 2048

Send/Receive NetFlow Data on Socket: 2055

Socket Receive Queue Size: 1000

Name Resolution

NetFlow Host Name Resolution: □

NetFlow Port Name Resolution: □

Version 9 Template

NetFlow v9 Template Refresh Rate (packets): 30

NetFlow v9 Template Timeout: 1 min(s)

Configuration

Enable NetFlow Collector

Select this checkbox to enable NetFlow packet processing on the Extreme Management Center server. Deselecting this checkbox disables all other fields in this panel and turns off NetFlow for troubleshooting purposes. Whether NetFlow is enabled or disabled, a message is logged to the event log as well as the Extreme Management Center server log. When NetFlow is disabled, the Application Flows report on the Flows tab is cleared.

Flow Collector Filter

Use this field to filter all incoming flows as they are processed by the flow collector. Flows not matching the filter are discarded and not maintained in memory on the server. If you add a filter here, the current flows stored in the cache are trimmed to only include matching flows.

Use this option if you want to use flow collection to look for specific results, but not process unrelated flows. For example, to only process flows pertaining to a particular subnet.

Export Interval

This is the active timer that determines the maximum amount of time a long-lasting flow remains active before expiring. When a long-lasting active flow expires due to the active timer expiring, another flow is immediately created to continue the ongoing flow. The Extreme Management Center flow collector rejoins these multiple flow records to report a single logical flow.

Maximum Aggregate Flows to Maintain in Memory

This indicates the amount of memory used to store aggregated flows.

Maximum Flows to Maintain in Memory

This indicates the amount of memory used to store flows.

Maximum Number of Flows Allowed per Table View

This indicates the maximum number of flows displayed in NetFlow reports.

Throttle Flows When Maximum Exceeded By (percent)

Flow collection is throttled when the Maximum Flows to Maintain in Memory is exceeded by the percentage entered here.

Worker Thread Queue Size

Decoded flow records are put into one of several fixed-size queues for processing. If the decoding rate exceeds the processing rate, the queue may overflow. This option allows you to configure the queue size (number of flow records).

Alarm Dispatcher

Flow Alarm Service Period

This controls how often the queue is checked for matched flows to process. The dispatcher runs once every service period. So by default, the dispatcher processes matches every 5 seconds.

Maximum Flow Alarm Queue Size

The maximum number of matched flows queued. By default, the dispatcher drops matched flows after 1000 matches are queued.

Maximum Flow Alarms Serviced Each Period

The maximum number of matched flows pulled from the queue for processing during a service period. By default, the dispatcher processes 100 matches every service period.

Socket

NetFlow Socket Buffer Size (bytes)

The buffer size (in bytes) set aside by the Extreme Management Center server for buffering incoming flows.

NetFlow Socket Data Size (bytes)

The socket data size in bytes. Do not change this setting unless it is required on your network.

Send/Receive NetFlow Data on Socket

The port on the Extreme Management Center server that listens for flow collection data. If you change this port number here, you also need to reconfigure the port number on the switch.

Socket Receive Queue Size

Network packets are retrieved from a datagram socket and put into a fixed-size queue for decoding into flow records. The queue can overflow if the receive rate exceeds the decoding rate. This option allows you to configure the queue size (number of network packets).

Name Resolution

NetFlow Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option enables host name resolution for NetFlow only. Host name resolution for Extreme Management Center is enabled globally using the Extreme Management Center Name Resolution option. The Name Resolution option must also be enabled for this NetFlow option to take effect.

NetFlow Port Name Resolution

Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to disable port name resolution for NetFlow only. (Port name resolution is enabled globally using the Name Resolution option.)

Version 9 Template

NetFlow v9 Template Refresh Rate (packets)

The number of export packets the flow sensor sends before retransmitting a template to the collector when using NetFlow Version 9.

NetFlow v9 Template Timeout

The amount of time the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.

Network Monitor Cache Options

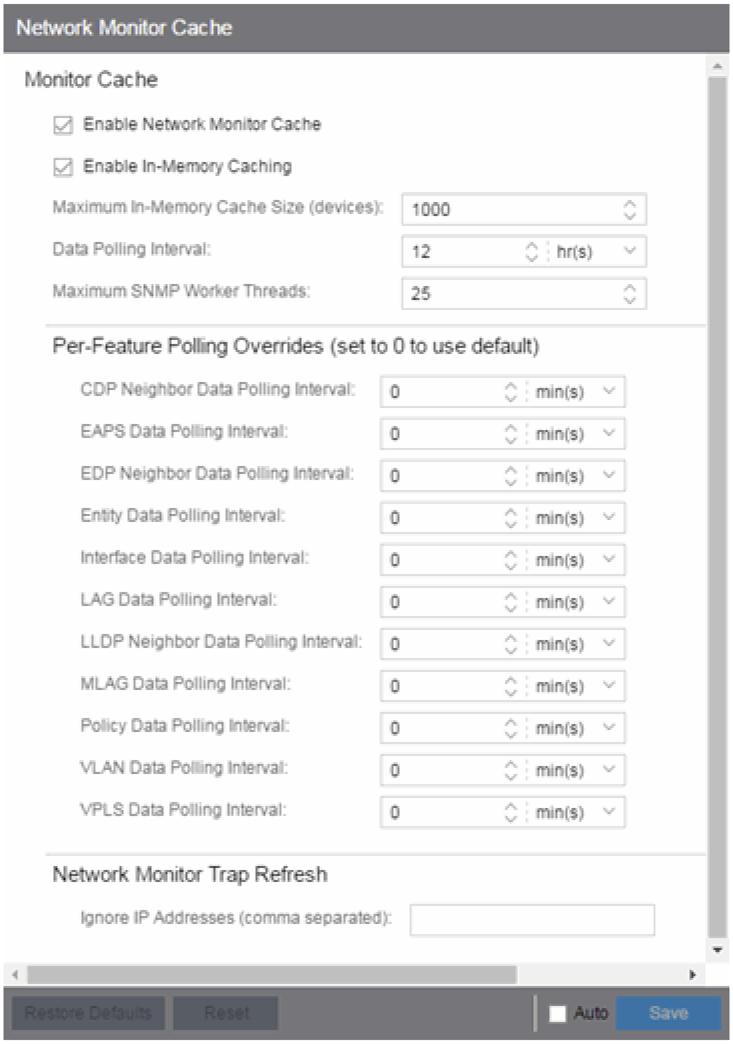
Selecting Network Monitor Cache in the left panel of the **Options** tab provides the following view, where you can edit network monitor cache settings. The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from multiple places including slot and port details (Entity, ifTable), default role (Policy), neighbor link details (CDP, EDP, LLDP), Ethernet Automatic Protection Switching (EAPS), and Multi System Link Aggregation (MLAG).

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

The cache is maintained in a two-tiered structure: device physical data is cached to the database and a fast in-memory cache maintains a subset of this data in memory on the server. The in-memory cache may contain all or a subset of devices stored in the database.

On the specified polling interval, the data is validated and automatically updated as necessary. Decreasing the poll interval increases background SNMP performed by the server.

Storing this information greatly improves performance for views in Extreme Management Center that request it. Enable the cache for the best experience.



Network Monitor Cache

Monitor Cache

☑ Enable Network Monitor Cache

☑ Enable In-Memory Caching

Maximum In-Memory Cache Size (devices): 1000

Data Polling Interval: 12 hr(s)

Maximum SNMP Worker Threads: 25

Per-Feature Polling Overrides (set to 0 to use default)

CDP Neighbor Data Polling Interval: 0 min(s)

EAPS Data Polling Interval: 0 min(s)

EDP Neighbor Data Polling Interval: 0 min(s)

Entity Data Polling Interval: 0 min(s)

Interface Data Polling Interval: 0 min(s)

LAG Data Polling Interval: 0 min(s)

LLDP Neighbor Data Polling Interval: 0 min(s)

MLAG Data Polling Interval: 0 min(s)

Policy Data Polling Interval: 0 min(s)

VLAN Data Polling Interval: 0 min(s)

VPLS Data Polling Interval: 0 min(s)

Network Monitor Trap Refresh

Ignore IP Addresses (comma separated):

Monitor Cache

Enable Network Monitor Cache

Select this option to enable the network monitor cache. Enabling the cache improves performance for Extreme Management Center views that request this information. Deselecting this option disables all other fields in this panel.

Enable In-Memory Caching

Select this option to enable the in-memory cache. To limit memory usage, disable the in-memory cache and configure the device cache to rely directly on the database.

Maximum In-Memory Cache Size (devices)

If Enable In-Memory Caching is enabled, enter the maximum number of devices whose data is stored in the in-memory cache. This option lets you adjust the amount of memory the cache uses.

Data Polling Interval

Enter the frequency that the device data is checked for changes. If the device data is stale, the data is refreshed in the cache. Reducing the interval increases background SNMP queries performed by the server.

Maximum SNMP Worker Threads

Enter the maximum number of threads that send SNMP queries in parallel if multiple devices are added to the cache at the same time. The cache is populated with results from SNMP queries to devices.

Per-Feature Polling Overrides

Use the fields in this section to set unique polling intervals for individual cache features polled more frequently. Set to 0 to use the default interval set for the Data Polling Interval.

Network Monitor Trap Refresh

Ignore IP Addresses (comma separated)

Enter a comma-separated list of the IP addresses for which you do not want Extreme Management Center to be the trap destination.

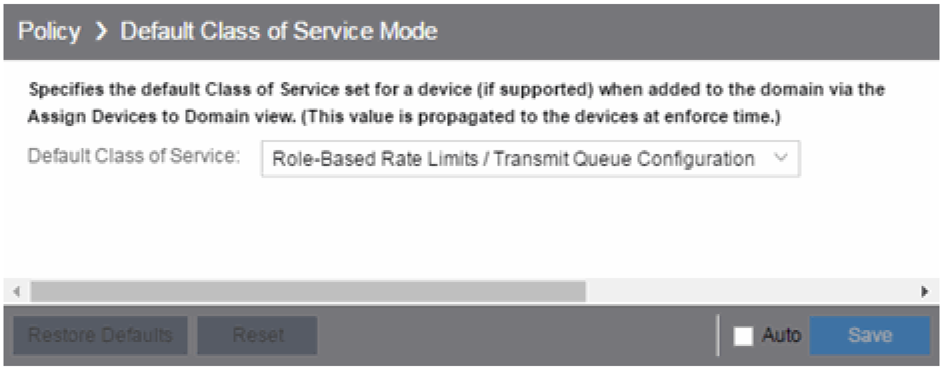
Policy Options

Selecting Policy in the left panel of the **Options** tab provides the following view, where you can edit options that apply to policy functionality found in the Policy tab and in the legacy Policy Manager java application.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Default Class of Service Mode

The **Default Class of Service** option allows you to specify the default Class of Service (CoS) mode to set on a device (if supported) when it is created in Extreme Management Center or added to the domain via the **Policy** tab. The default setting is **Role-Based Rate Limits/ Transmit Queue Configuration**. The CoS mode is written to the devices when an Enforce operation is performed. This setting applies to all users.


Policy > Default Class of Service Mode

Specifies the default Class of Service set for a device (if supported) when added to the domain via the Assign Devices to Domain view. (This value is propagated to the devices at enforce time.)

Default Class of Service: Role-Based Rate Limits / Transmit Queue Configuration

Select the CoS mode or select the option to disable rate limits on devices. Only certain devices such as the N-Series Gold and Platinum devices support both modes, but you cannot enable both at the same time. For additional information, see Getting Started with Class of Service.

Rate Limits Disabled

Select this mode to disable rate limits. This means that any priority-based rate limits are not written to devices on enforce, and any role-based rate limits are not included in roles written to devices on enforce.

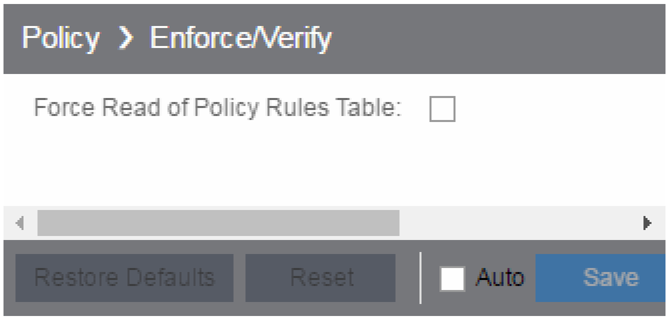
Role-Based Rate Limits/Transmit Queue Configuration

Select this mode to configure role-based rate limits and transmit queues on devices. These rate limits are defined within a CoS and are associated with a specific role via a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the CoS. For additional information, see How to Define Rate Limits and How to Configure Transmit Queues.

Priority-Based Rate Limits

Priority-based rate limits are supported in Extreme Management Center for use with legacy devices such as the E7 and E1 devices. For additional information, see Priority-Based Rate Limits.

Enforce/Verify



Policy > Enforce/Verify

Force Read of Policy Rules Table: □

Force Read of Policy Rules Table

To improve performance during the verify operation, Extreme Management Center uses the "Last Changed" attribute on the device to determine if any rules changed. Selecting the **Force Read of Policy Rules Table** option causes Extreme Management Center to perform the verify operation using the rules table instead of the attribute. This may cause the verify operation to take longer to perform. Do not select this option unless instructed by Extreme Networks Support.

Related Information

For information on related topics:

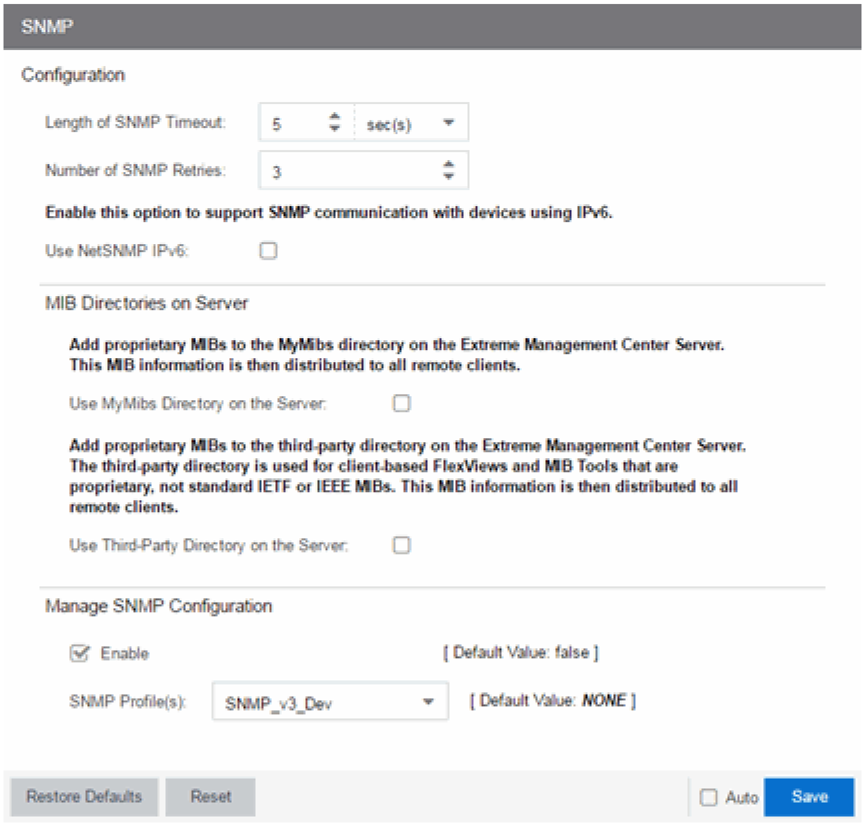
- Policy

SNMP Options

Selecting SNMP in the left panel of the **Options** tab provides the following view, which allows you to configure SNMP options.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

These options apply to all users. For these settings to take effect, the Extreme Management Center Server must be restarted.



SNMP

Configuration

Length of SNMP Timeout: 5 sec(s)

Number of SNMP Retries: 3

Enable this option to support SNMP communication with devices using IPv6.

Use NetSNMP IPv6: □

MIB Directories on Server

Add proprietary MIBs to the MyMibs directory on the Extreme Management Center Server. This MIB information is then distributed to all remote clients.

Use MyMibs Directory on the Server: □

Add proprietary MIBs to the third-party directory on the Extreme Management Center Server. The third-party directory is used for client-based FlexViews and MIB Tools that are proprietary, not standard IETF or IEEE MIBs. This MIB information is then distributed to all remote clients.

Use Third-Party Directory on the Server: □

Manage SNMP Configuration

☑ Enable [Default Value: false]

SNMP Profile(s): SNMP_v3_Dev [Default Value: *NONE*]

Configuration

Length of SNMP Timeout

The amount of time Extreme Management Center waits before trying to contact a device again. The default value for this setting is 5 seconds. The value for this setting must be between 1 and 60 seconds.

Override this value on a per-device basis in the **SNMP Timeout** field in the Configure Device window.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

Number of SNMP Retries

The number of attempts made to contact a device after an attempt at contact fails. The default setting is 3 retries, which means that Extreme Management Center retries a timed-out request three times after the initial attempt at contact is made, making a total of four attempts to contact a device. The value for this setting must be between 1 and 10 retries.

Override this value on a per-device basis in the **SNMP Retries** field in the Configure Device window.

Use NetSNMP IPv6

The **Use NetSNMP IPv6** option allows you to use SNMP to manage network devices to which IPv6 addresses are assigned. You must have this option selected in order to be able to add a device with an IPv6 address.

MIB Directories on Server

Use MyMibs Directory on the Server

Select this checkbox to allow the Extreme Management Center Server to also use the MyMibs directory (e.g. the MIBs are included in the SNMP server stack). This MIB information is then distributed to the Extreme Management Center remote clients.

Use Third-Party Directory on the Server

Select this checkbox to allow the Extreme Management Center Server to also use the third-party directory, where proprietary, client-based FlexViews and MIB Tools (Enterprise MIBs owned by other companies) are stored, not standard IETF or IEEE MIBs. This MIB information is then distributed to the Extreme Management Center remote clients.

CAUTION: Do **not** use the MyMibs or third-party directories unless it is required on your network, as selecting these options may cause Extreme Management Center Server instability and undesirable consequences.

Manage SNMP Configuration

Enable

Select this checkbox to allow access to the Extreme Management Center and Extreme Access Control engines for the profiles you select in the **SNMP Profile(s)** drop-down menu.

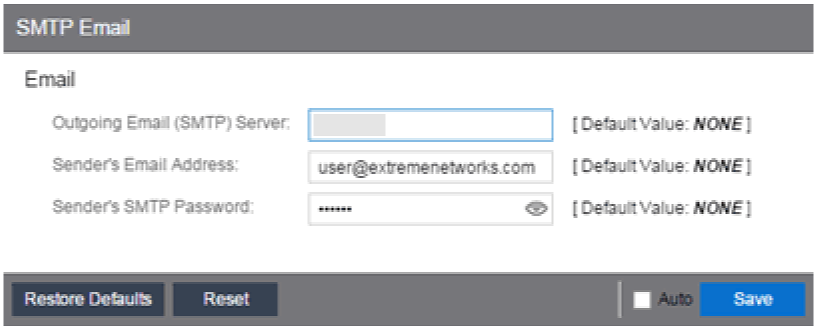
SNMP Profile(s)

Select the profiles with access to the Extreme Management Center and Extreme Access Control engines. The type of access (e.g. read-only or read-write) is configured for the profile by assigning a set of SNMP credentials to the profile on the Administration > Profiles tab.

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.



SMTP Email

Email

Outgoing Email (SMTP) Server: [Default Value: *NONE*]

Sender's Email Address: user@extremenetworks.com [Default Value: *NONE*]

Sender's SMTP Password: •••••• [Default Value: *NONE*]

Outgoing Email (SMTP) Server

Identifies the email server used for outgoing messages.

Sender's Email Address

The sender's email address used to send outgoing email notification messages. Enter the address in a fully qualified format, such as "sender's name@sender's domain."

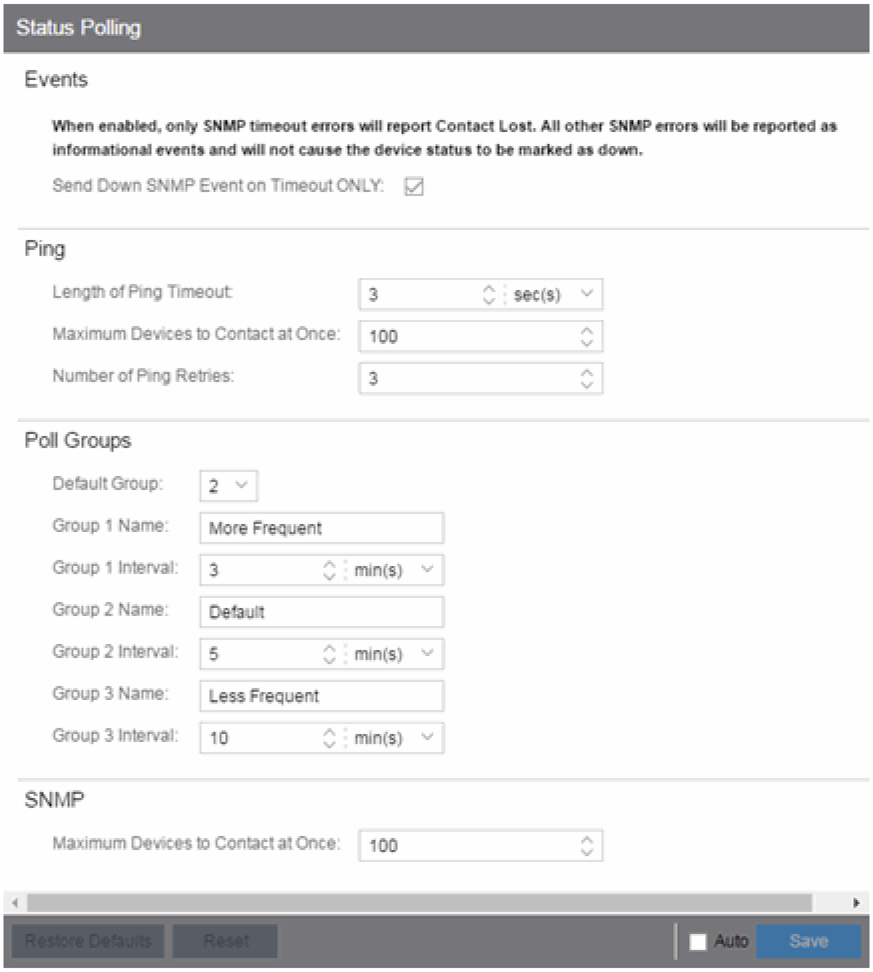
Sender's SMTP Password

The password for the user account entered in the **Sender's Email Address** field. Select the **Eye** icon to display your password.

Status Polling Options

Selecting Status Polling in the left panel of the **Options** tab provides the following view, where you can specify options that determine how Extreme Management Center polls devices. Extreme Management Center uses the polling options and poll groups defined here to contact the devices and update tree information. When a device is added to the Extreme Management Center database using the Add Device menu option or a device discover, it is added to the default poll group selected here. (A device discover lets you assign devices to any of the three poll groups.) Reassign individual devices or device groups to a different poll group using the Configure Device window. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Status Polling

Events

When enabled, only SNMP timeout errors will report Contact Lost. All other SNMP errors will be reported as informational events and will not cause the device status to be marked as down.

Send Down SNMP Event on Timeout ONLY: ☑

Ping

Length of Ping Timeout: 3 sec(s)

Maximum Devices to Contact at Once: 100

Number of Ping Retries: 3

Poll Groups

Default Group: 2

Group 1 Name: More Frequent

Group 1 Interval: 3 min(s)

Group 2 Name: Default

Group 2 Interval: 5 min(s)

Group 3 Name: Less Frequent

Group 3 Interval: 10 min(s)

SNMP

Maximum Devices to Contact at Once: 100

Events

When the **Send Down SNMP Event on Timeout ONLY** option is selected, only SNMP timeout errors result in a **Contact Lost** device status. All other SNMP errors are reported as informational events in the Alarms and Events > Events tab and do not cause the device status to be marked as "down" with a red down arrow.

Ping

These status polling options pertain to devices whose poll type is set to **Ping**.

Length of Ping Timeout

The amount of time Extreme Management Center waits before trying to ping a device again. The default setting is 3 seconds. The maximum value for this field is 60 seconds.

Maximum Devices to Contact at Once

The maximum number of IP addresses that Extreme Management Center attempts to contact simultaneously. The maximum value for this field is 1,000.

Number of Ping Retries

The number of attempts made to ping a device. The default setting is 3 retries, which means Extreme Management Center retries a timed-out request three times, making a total of four attempts to contact a device. The maximum value for this field is 10.

Poll Groups

There are three distinct poll groups, and each device belongs to one of the three groups. This lets you poll critical devices at a more frequent interval, while polling non-essential devices less frequently. The poll frequency for each group specifies the actual length of the poll cycle. Set the interval for poll groups according to your network's needs using the guidelines below.

Select one group as the default poll group in the **Default Group** drop-down menu. When a device is added to the Extreme Management Center database using the Add Device menu option or a CDP seed IP discover, it is added to the default poll group selected here. (IP range discover lets you assign devices to any of the three poll groups.) You can also assign individual devices or device groups to a specific poll group using the Configure Device window.

The overall density of polling for devices whose poll type is set to Ping and SNMP is controlled by the **Maximum Devices to Contact at Once** setting in the Ping and SNMP section, respectively. This determines the maximum number of devices from each group polled at any given time. Extreme Management Center always attempts to poll up to the maximum number of devices until all of the devices in the three groups are polled. As responses are received and devices are removed from the poll queue, other devices are added to the queue. Once all the devices are polled, Extreme Management Center stops polling and batches information to update clients.

If the **Maximum Devices to Contact at Once** is set too high, such that the poll density is too high, system performance degrades quickly. The optimal poll setting is dependent on many factors including, but not limited to, CPU speed, RAM, and network devices. As the number of devices that you are polling increases, reduce the poll density (**Maximum Devices to Contact at Once**) to increase performance.

The default **Maximum Devices to Contact at Once** setting and poll group intervals provided as defaults are a good starting point. If necessary, adjust the values to optimize status polling for your network.

SNMP

This status polling option pertains to devices whose poll type is set to **SNMP**.

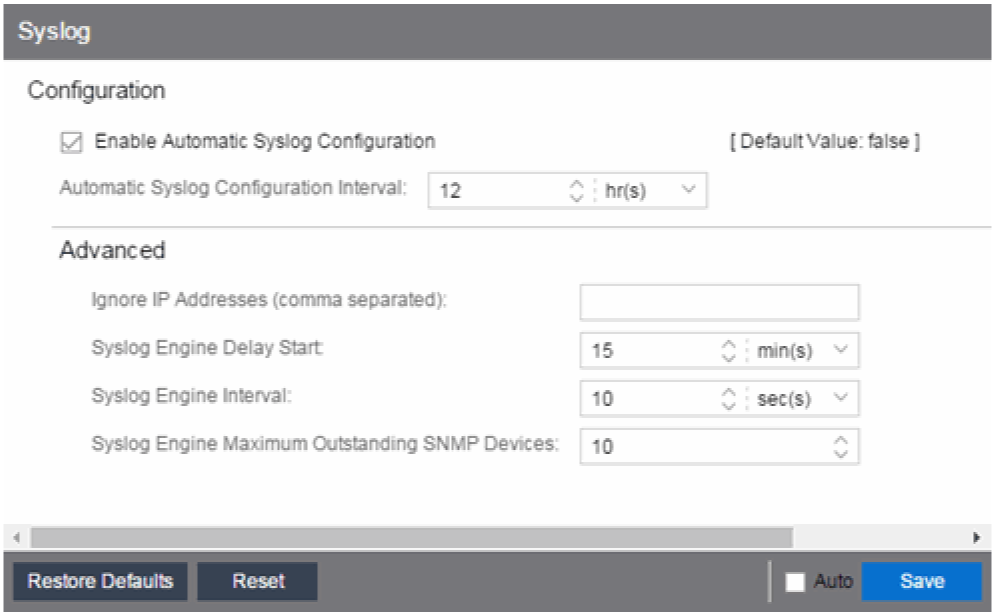
Maximum Devices to Contact at Once

The maximum number of IP addresses that Extreme Management Center attempts to contact simultaneously. The maximum value for this field is 1,000.

Syslog Options

Selecting Syslog in the left panel of the **Options** tab provides the following view, where you can set Extreme Management Center to automatically configure devices to send syslog information.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Syslog

Configuration

☑ Enable Automatic Syslog Configuration [Default Value: false]

Automatic Syslog Configuration Interval: 12 hr(s)

Advanced

Ignore IP Addresses (comma separated):

Syslog Engine Delay Start: 15 min(s)

Syslog Engine Interval: 10 sec(s)

Syslog Engine Maximum Outstanding SNMP Devices: 10

Enable Automatic Syslog Configuration
Select the checkbox to configure Extreme Management Center to automatically gather information and post it to the syslog. Deselecting this option disables the **Automatic Syslog Configuration Interval** field.

Automatic Syslog Configuration Interval
Enter the frequency with which Extreme Management Center automatically gathers information and posts it to the syslog.

Ignore IP Addresses (comma separated)
Enter any IP addresses you do not want automatically logged to the syslog.

Syslog Engine Delay Start
The amount of time Extreme Management Center waits before information in the syslog is aggregated and archived.

Syslog Engine Interval

The amount of time Extreme Management Center waits before checking whether a device is properly configured to send syslog information. If the device is not properly configured and Enable Automatic Syslog Configuration is selected, Extreme Management Center automatically configures the device.

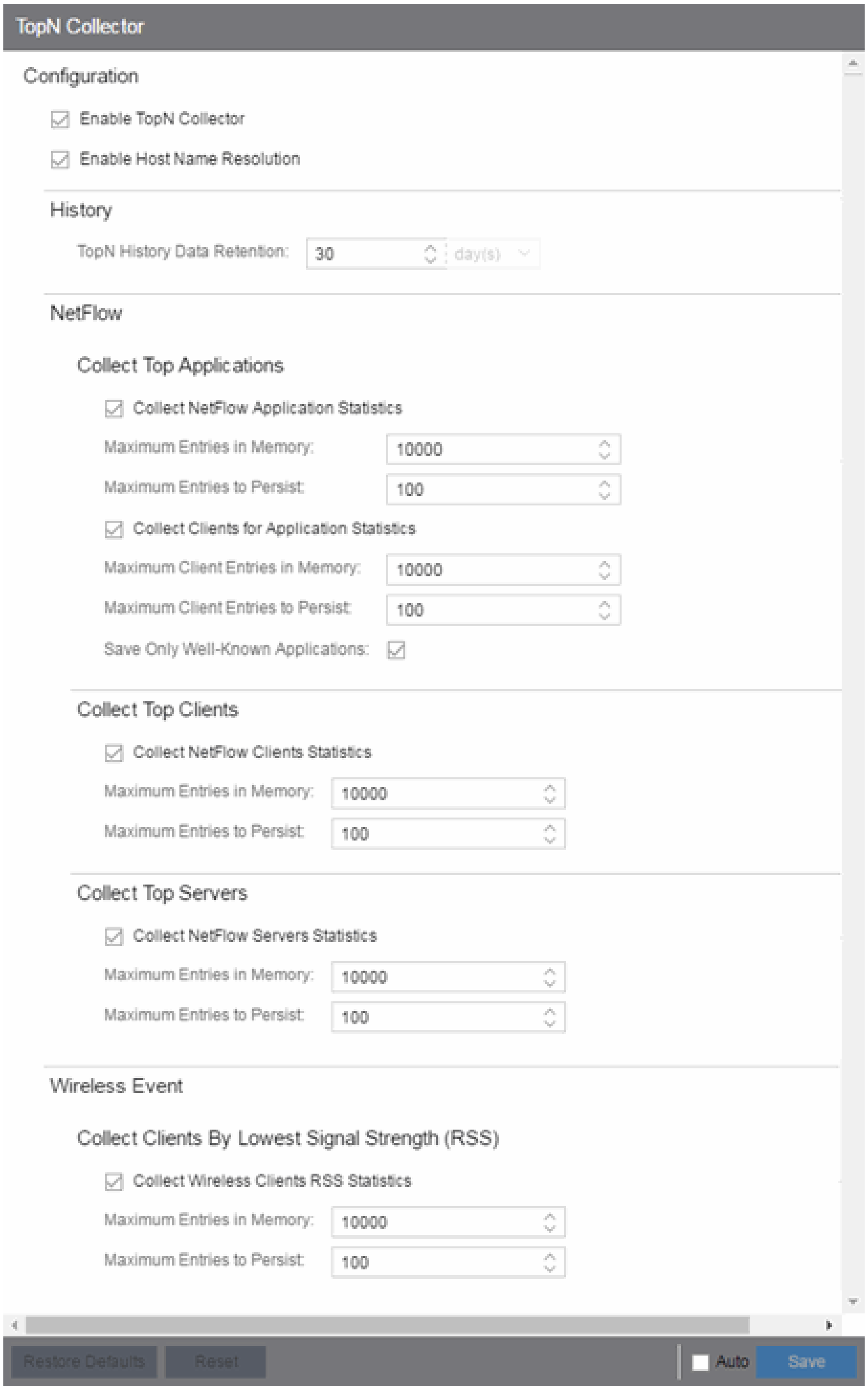
Syslog Engine Maximum Outstanding SNMP Devices

The maximum number of outstanding SNMP devices archived by the syslog.

TopN Collector Options

Selecting TopN Collector in the left panel of the **Options** tab provides the following view, where you can enable the TopN collector and host name resolution, and configure the number of days Extreme Management Center maintains the TopN history. The TopN Collector gathers the application, client application, client, and server data used in TopN reports. It also collects the signal strength data reported by Wireless Controllers.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



TopN Collector

Configuration

☑ Enable TopN Collector

☑ Enable Host Name Resolution

History

TopN History Data Retention: 30 day(s)

NetFlow

Collect Top Applications

☑ Collect NetFlow Application Statistics

Maximum Entries in Memory: 10000

Maximum Entries to Persist: 100

☑ Collect Clients for Application Statistics

Maximum Client Entries in Memory: 10000

Maximum Client Entries to Persist: 100

Save Only Well-Known Applications: ☑

Collect Top Clients

☑ Collect NetFlow Clients Statistics

Maximum Entries in Memory: 10000

Maximum Entries to Persist: 100

Collect Top Servers

☑ Collect NetFlow Servers Statistics

Maximum Entries in Memory: 10000

Maximum Entries to Persist: 100

Wireless Event

Collect Clients By Lowest Signal Strength (RSS)

☑ Collect Wireless Clients RSS Statistics

Maximum Entries in Memory: 10000

Maximum Entries to Persist: 100

Enable TopN Collection

Select this option to enable the TopN Collector. Deselecting this option disables all other fields in the panel. Changes to this option take place immediately.

Enable Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for TopN only. (Host name resolution is enabled globally using the Enable Name Resolution option.) Changes to this option take place immediately.

History

TopN History Data Retention

This setting determines the number of days TopN information remains available for viewing in reports. The default number of days is 30, with a minimum value of 1 day and a maximum value of 180 days. Changes to this option take effect with the next nightly TopN history cleanup task performed by the Extreme Management Center server.

NetFlow

The TopN Collector collects the data used in TopN reports for applications, client applications, clients, and servers. The collector collects data over a one hour time period. At the end of the hour, the collector evaluates the data and stores only the most significant details collected for that hour. When changing the value for **Maximum Entries in Memory** or **Maximum Entries to Persist**, the new value takes effect during the next hour of data collection. For example, if you change the value at 3:05 or 3:55, the new value takes effect during the hour that starts at 4:00.

If more entries are needed during the hour than the maximum, additional entries are stored on disk, which is slower. This results in a direct trade-off in memory usage versus CPU usage. Increasing these values might use more memory and decreasing these values might use more CPU.

Collect Top Applications

Collect NetFlow Application Statistics

Select this checkbox to enable the collection of application TopN data.

Maximum Entries in Memory

Specify the number of application entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of application entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Clients for Application Statistics

Select this checkbox to enable the collection of data about the clients using the applications in TopN data.

Maximum Client Entries in Memory

Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Client Entries to Persist

Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Save Only Well-Known Applications

Select this checkbox to save only data from well-known applications in the TopN data.

Collect Top Clients

Collect NetFlow Clients Statistics

Select this checkbox to enable the collection of client TopN data.

Maximum Entries in Memory

Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Top Servers

Collect NetFlow Servers Statistics

Select this checkbox to enable the collection of server TopN data.

Maximum Entries in Memory

Specify the number of server entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of server entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Wireless Event

Collect Wireless Clients RSS Statistics

Select this checkbox to enable Wireless Controllers to collect signal strength data for TopN reporting.

Maximum Entries in Memory

Specify the number of signal strength entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

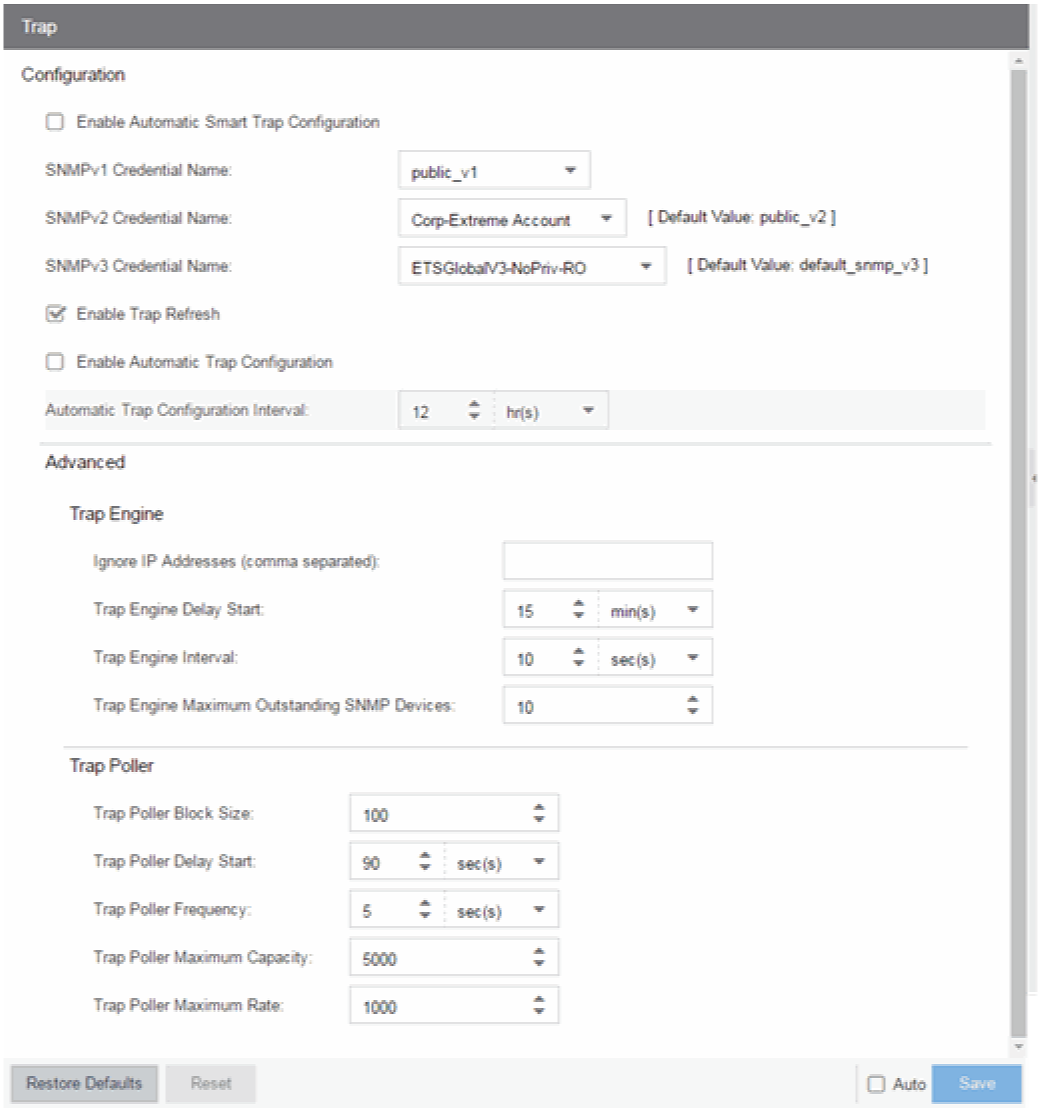
Specify the number of signal strength entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Trap Options

Selecting Trap in the left panel of the **Options** tab provides the following view, where you can set trap options for Extreme Management Center.

SNMP traps are messages a device sends to Extreme Management Center to indicate its status. Using traps, a network manager can monitor a large number of devices simultaneously without needing to poll them individually.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Trap

Configuration

□ Enable Automatic Smart Trap Configuration

SNMPv1 Credential Name: public_v1

SNMPv2 Credential Name: Corp-Extreme Account [Default Value: public_v2]

SNMPv3 Credential Name: ETSGlobalV3-NoPriv-RO [Default Value: default_snmp_v3]

☑ Enable Trap Refresh

□ Enable Automatic Trap Configuration

Automatic Trap Configuration Interval: 12 hr(s)

Advanced

Trap Engine

Ignore IP Addresses (comma separated):

Trap Engine Delay Start: 15 min(s)

Trap Engine Interval: 10 sec(s)

Trap Engine Maximum Outstanding SNMP Devices: 10

Trap Poller

Trap Poller Block Size: 100

Trap Poller Delay Start: 90 sec(s)

Trap Poller Frequency: 5 sec(s)

Trap Poller Maximum Capacity: 5000

Trap Poller Maximum Rate: 1000

Configuration

Use this section to configure traps to be automatic traps or automatic smart traps. Additionally, you can configure the amount of time in hours between automatic trap configurations as well as select credential names.

Enable Automatic Smart Trap Configuration

Select this option to allow your ExtremeXOS devices to send Extreme Management Center a trap when a change occurs on the device.

SNMPv1 Credential Name

Select the SNMPv1 credentials used to access the device. You can modify the credentials found in this list in the SNMP Credentials section on the Administration > Profiles tab.

SNMPv2 Credential Name

Select the SNMPv2 credentials used to access the device. You can modify the credentials found in this list in the SNMP Credentials section on the Administration > Profiles tab.

SNMPv3 Credential Name

Select the SNMPv3 credentials used to access the device. You can modify the credentials found in this list in the SNMP Credentials section on the Administration > Profiles tab.

Enable Trap Refresh

Select this option to allow Extreme Management Center to refresh information on the devices when the trap is received.

Enable Automatic Trap Configuration

Select this option to configure the ExtremeXOS switches on your network to send Extreme Management Center traps using the SNMP credentials specified in the SNMP Credential Name fields. Devices on which Automatic Trap Configuration is enabled are polled at the interval specified in Automatic Trap Configuration Interval.

Automatic Trap Configuration Interval

Select the frequency with which your devices send SNMP traps to Extreme Management Center.

Trap Engine

Use this section to enter a list of IP addresses that should be ignored by traps and to configure trap engine options.

Ignore IP Addresses (comma separated)

Enter a comma-separated list of IP addresses of the devices from which the trap engine ignores traps.

Trap Engine Delay Start

Select the amount of time after starting the trap engine to delay receiving traps.

Trap Engine Interval

Select the frequency with which the trap engine collects SNMP traps from devices.

Trap Engine Maximum Outstanding SNMP Devices

Select the maximum number of SNMP devices that send traps to the trap engine.

Trap Poller

Use this section to set advanced options for polling traps.

Trap Poller Block Size

Select the number of traps the trap engine maintains at one time.

Trap Poller Delay Start

Select the amount of time after starting the trap engine that devices are polled by Extreme Management Center.

Trap Poller Frequency

Select the frequency with which the trap engine polls devices.

Trap Poller Maximum Capacity

Select the maximum number of devices the trap engine polls for traps.

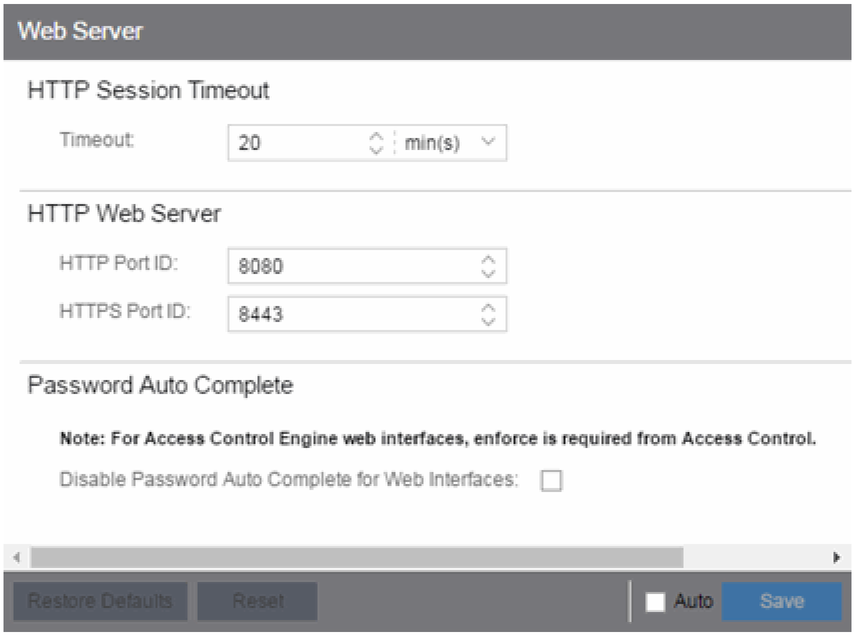
Trap Poller Maximum Rate

Select the maximum number of devices the trap engine polls at one time.

Web Server Options

Selecting Web Server in the left panel of the **Options** tab provides the following view, where you can specify web browser options when using Extreme Management Center.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



HTTP Session Timeout

Timeout: 20 min(s)

HTTP Web Server

HTTP Port ID: 8080

HTTPS Port ID: 8443

Password Auto Complete

Note: For Access Control Engine web interfaces, enforce is required from Access Control.

Disable Password Auto Complete for Web Interfaces: □

HTTP Session Timeout

The **Timeout** option lets you specify a session timeout value for all Extreme Management Center web-based views.

HTTP Port ID

The **HTTP Port ID** field lets you specify the HTTP port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8080. If you change the port ID, you must restart the Extreme Management Center Server for the change to take effect.

IMPORTANT: Enforce your Extreme Access Control engines via the **Control** > Extreme Access Control tab immediately after changing the **HTTP Port ID**. Do not change the **HTTPS Port ID** until after you enforce.

When adding a new Extreme Access Control engine, the **HTTP Port ID** must be **8080**.

HTTPS Port ID

The **HTTPS Port ID** field lets you specify the HTTPS port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8443. If you change the port ID, you must restart the Extreme Management Center Server for the change to take effect.

IMPORTANT: Do not change the HTTP Port ID for at least one minute after changing the HTTPS Port ID to ensure Extreme Management Center polls the Extreme Access Control engine.

When adding a new Extreme Access Control engine, the **HTTPS Port ID** must be **8443**.

Password Auto Complete

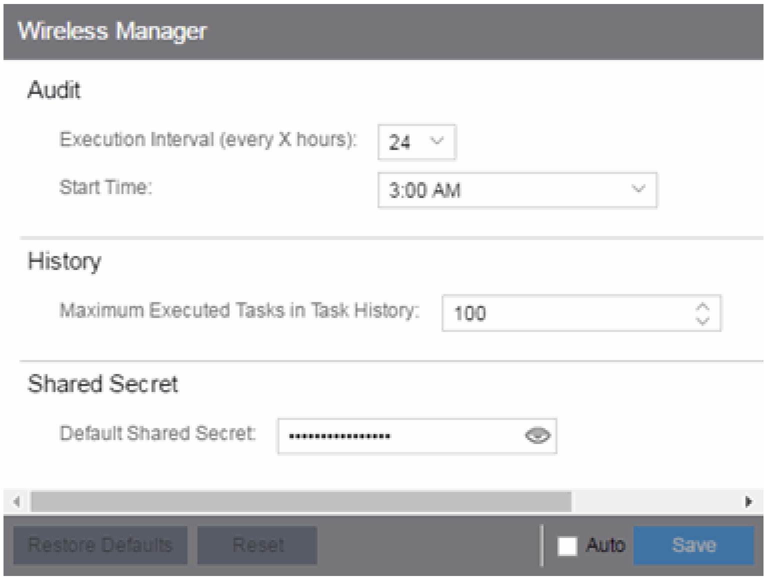
The **Disable Password Auto Complete for Web Interfaces** option lets you disable automatic password completion for users logging into Extreme Management Center web interfaces. Note that for Extreme Access Control web interfaces, you must enforce from the **Control** > Extreme Access Control tab for the option to take effect.

These settings apply to all users. You must be assigned the appropriate user capability to change this setting.

Wireless Manager Options

Selecting Wireless Manager in the left panel of the **Options** tab provides the following view, where you can specify options for the Wireless Manager application.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Wireless Manager

Audit

Execution Interval (every X hours): 24

Start Time: 3:00 AM

History

Maximum Executed Tasks in Task History: 100

Shared Secret

Default Shared Secret: ••••••••••••••••••

Wireless Manager audits controller configurations to ensure that it does not deviate from the deployed templates. When Wireless Manager encounters discrepancies between the template and the actual controller configuration, the audit feature logs an error. You can manually run an audit or you can schedule automatic audits using these Audit options.

Execution Interval (every X hours)

Use the drop-down menu to select the interval in hours between the start of successive audits. Auditing once every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

Start Time

Use the drop-down menu to select the time when the audit starts.

Maximum Executed Tasks in Task History

Enter the number of Wireless Manager tasks you want to save in the Wireless Manager database. Enter 0 if you do not want to execute a Wireless Manager audit.

After a task has executed, it is retained in the Wireless Manager database to provide a detailed history of task activity. A large amount of information is kept for each executed task, including the complete CLI script executed against each target controller. To maintain the database at a reasonable size, Wireless Manager keeps only a fixed number of executed tasks in the database. When the task limit is reached or exceeded, Wireless Manager deletes the oldest executed tasks from its database. The History option allows you to control how many task definitions Wireless Manager retains in its database. The default is 100 executed tasks retained, and the maximum is 500 tasks retained.

Default Shared Secret

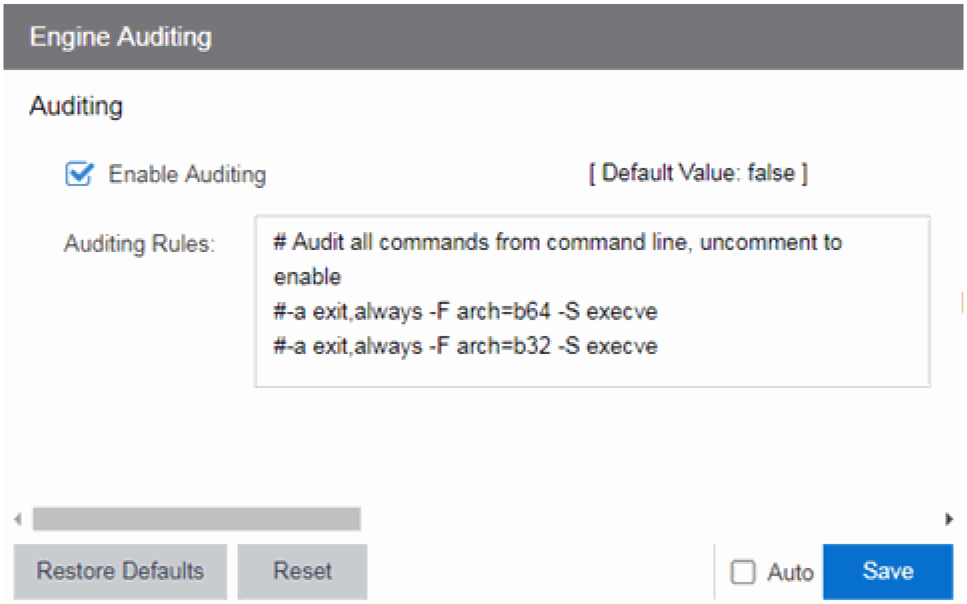
Enter a Shared Secret, which is a password used by Extreme Management Center to authenticate with the controller.

When Extreme Management Center discovers a new controller, Wireless Manager attempts to authenticate with the controller using this shared secret. For proper functioning, Extreme Management Center and the controller must be configured with the same shared secret. Each controller can be configured with a different Shared Secret as long as Wireless Manager knows what it is. You can configure a Shared Secret on a per controller basis using Wireless Manager. Select the Eye icon to display your password. For additional information, see Shared Secrets Page.

Engine Auditing Options

Selecting Engine Auditing in the left panel of the **Options** tab provides the following view, where you can enable auditing of users connected to the Extreme Management Center server CLI via SSH.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



☑ Enable Auditing [Default Value: false]

Auditing Rules:

```
# Audit all commands from command line, uncomment to
enable
#-a exit,always -F arch=b64 -S execve
#-a exit,always -F arch=b32 -S execve
```

☐ Auto

Enable Auditing

Selecting the **Enable Auditing** option enables the **Auditing Rules** field, where you can configure Extreme Management Center to store all commands entered by users connected to the Extreme Management Center CLI via SSH in the syslog file.

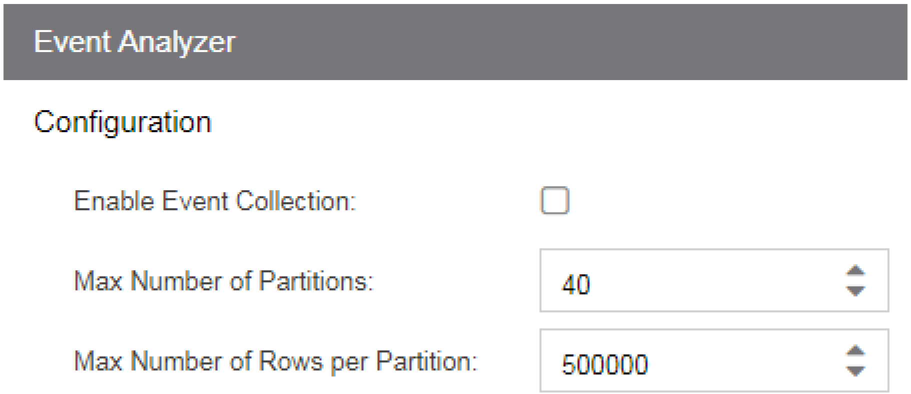
Auditing Rules

Remove the # symbol from the beginning of a command line to enable the command and store user commands entered using the Extreme Management Center CLI.

Event Analyzer Options

Selecting Event Analyzer in the left panel of the **Options** tab provides the following view, where you can configure the settings related to the Event Analyzer in Extreme Management Center.

Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.



Event Analyzer

Configuration

Enable Event Collection: □

Max Number of Partitions: 40

Max Number of Rows per Partition: 500000

Enable Event Collection

Selecting the **Enable Event Collection** option saves wireless client events and enables Event Analyzer tab functionality so that the tab populates with live data.

> **NOTE:** Enabling Event Collection uses a large amount of disk space, so this option is disabled by default.

Max Number of Partitions

Enter the maximum number of partitions used for the Event Analyzer.

> **NOTE:** Only change this value if you are an expert user.

Max Number of Rows per Partition

Enter the maximum number of rows for each partition used for the Event Analyzer.

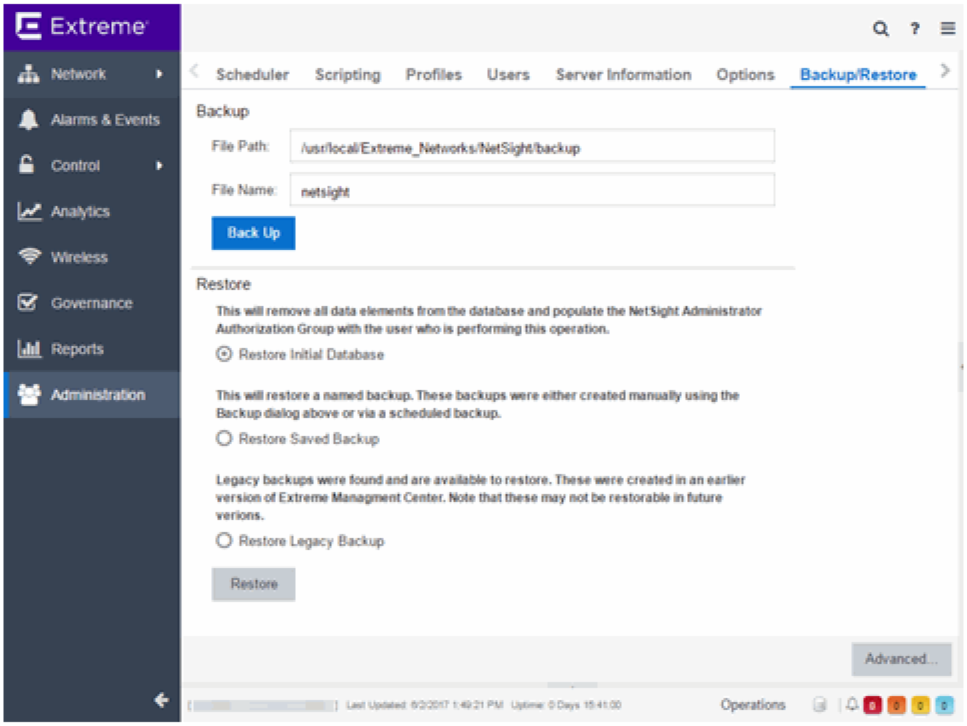
> **NOTE:** Only change this value if you are an expert user.

Backup/Restore

This tab allows you to save the currently active database as a file, restore the initial database or restore a saved legacy database, and manage the password and connection URL for the database. You must be assigned the appropriate user capabilities to perform these functions.

IMPORTANT: By default, version 8.1 of Extreme Management Center creates a binary database backup, which provides a more efficient method of backing up the database and uses less resources. The backup process functions identically to previous versions of Extreme Management Center.

Additionally, there are specific database backup migration requirements for this release.



Backup

File Path: /usr/local/Extreme_Networks/NetSight/backup

File Name: netsight

Restore

This will remove all data elements from the database and populate the NetSight Administrator Authorization Group with the user who is performing this operation.

● Restore Initial Database

This will restore a named backup. These backups were either created manually using the Backup dialog above or via a scheduled backup.

○ Restore Saved Backup

Legacy backups were found and are available to restore. These were created in an earlier version of Extreme Managment Center. Note that these may not be restorable in future verions.

○ Restore Legacy Backup

Last Updated: 6/2/2017 1:49:21 PM Uptime: 0 Days 15:41:00

Backup

Use the Backup section of the tab to save the current database. Specify a directory path in which to save the database backup as a file and name the file.

NOTE: To schedule regular database backups, use the Database Backup option available from Administration > Options > Database Backup.

File Path

Enter the path to the directory to which you want to save the file.

File Name

Enter a name for the database backup file.

Back Up

Starts the backup operation.

Restore

Use the Restore section to restore the initial database or restore a saved database. Both functions cause all current client connections and operations in progress to be terminated.

IMPORTANT: After restoring the Extreme Management Center server, enforce all Extreme Access Control engines.

Restore Initial Database

Select this option to remove all data elements from the database and populate the Extreme Management Center Administrator authorization group with the name of the logged-in user.

Restore Saved Backup

Select this option to remove all data elements from the database and then re-populate the database using a saved file created in version 8.0. Use the drop-down menu to select the file from which you want to populate the database.

NOTE: If there are no database backups saved (backups saved in version 8.0), this field does not display.

Restore Legacy Backup

Select this option to remove all data elements from the database and then re-populate the database using a saved backup file created before version 8.0. Use the drop-down menu to select the file from which you want to populate the database.

NOTE: If there are no legacy database backups saved (backups saved in version 7.1), this field does not display.

When restoring a saved legacy database to a new Extreme Management Center server installation, any memory or database configuration changes on the original server requires a manual change on the new server in order to replicate the configuration of the original Extreme Management Center server.

- Changes to the default -Xmx memory settings in the `<install directory>\services\nsserver.cfg` file needs to be duplicated on the new server when the database is restored. To change the memory setting to match the previous server, stop the Extreme Management Center server and edit the nsserver.cfg file.
- The mySQL my.ini file also needs to be manually updated to match any changes made on the original server.

Restore

Starts the restore operation.

Advanced

Displays the Advanced section of the window.

Advanced

Use the Advanced section of the tab to configure the URL and password the Extreme Management Center server uses when it connects to the database.

IMPORTANT: When Extreme Management Center is installed, it automatically secures the MySQL database server by removing all the root and anonymous users from the MySQL user database. Extreme Management Center then adds one generic user name (user = netsight) and password (password = enterasys). Change this password, as all customers who install Extreme Management Center know this generic password.

Connection URL

Displays the URL the Extreme Management Center server uses when connecting to the database. For troubleshooting purposes, (for example, if you can't connect to the database) you may wish to enter a new connection URL. Enter a new URL in the following format, and click **Apply**:
`jdbc:mysql://[hostname]/<database>` where [*hostname*] is optional.

NOTE: You must restart both the Extreme Management Center server and client after you change the **Connection URL**.

Password

Enter the password the Extreme Management Center uses when connecting to the database. Select the **Eye** icon to display your password.

NOTE: You must restart both the Extreme Management Center server and client after you change the **Connection URL**.

Restore Defaults

Restores the default values for the **Connection URL** and **Password** fields.

Reset

Discards any unsaved changes in the **Connection URL** and **Password** fields.

Save

Saves changes made to the **Connection URL** and **Password** fields.

Related Information

For information on related topics:

- Database Backup Options

Use the Options window (**Tools > Options**) to set Suite options that apply across all Extreme Management Center applications. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Suite folder in the tree to view the suite-wide options you can set.

Instructions on setting the following Suite options:

- Advanced SNMP Settings
- Advanced Suite Settings
- Alarm Configuration
- Alarm/Event Logs and Tables
- Client Connections
- Database Backup
- Data Display Format
- Date/Time Format
- Diagnostic Configuration
- ExtremeNetworks.com Update
- MAC OUI Vendor List
- Name Resolution
- NetSight Feedback Program
- NetSight Server Health
- Network Monitor Cache
- Port Monitor
- Services for NetSight Server
- SMTP E-Mail Server
- Status Polling
- System Browser
- Tree
- Web Server

Advanced SNMP Settings

The Advanced SNMP Settings view provides the option to have the NetSight Server use the MyMibs directory or thirdparty directory.

The MyMibs directory is where you add proprietary MIBs to the MIB database on the NetSight Server. This MIB information is then distributed to the NetSight remote clients. If you select this option, the NetSight Server will also use the MyMibs directory (e.g. the MIBs will be included in the SNMP Server Stack).

The third party directory is used for client-based FlexViews and MIB Tools that are proprietary (Enterprise MIBs owned by other companies), not standard IETF or IEEE MIBs. If you select this option, the NetSight Server will also use the third party directory.

CAUTION: In most situations, it is recommended that the NetSight Server should **not** use the MyMibs or thirdparty directories. However, the option is provided for situations where that behavior is warranted. Be aware that selecting this option could result in NetSight Server instability and undesirable consequences.

The Use NetSNMP IPv6 option allows you to SNMP-manage network devices that have IPv6 addresses assigned to them. You must have this option selected in order to be able to add a device with an IPv6 address.

These options apply to all users. For these setting to take effect, the NetSight Server must be restarted.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Advanced SNMP Settings.
3. Select the desired advanced SNMP options.
4. Click **OK** to set the option and close the window. Click **Apply** to set the option and leave the window open.
5. Restart the NetSight Server for these settings to take effect.

Advanced Suite Settings

The Advanced Suite Settings view provides the option to enable or disable NetSight Suite Beta Features. A list of the beta features can be found in the NetSight Suite Release Notes. When you enable the Beta features, you will be asked for a Beta Activation Key. Contact Extreme Networks Support to obtain a Beta Key. Once you enable the beta features, the button will change to "Disable Beta Features."

This option applies to all users. For this setting to take effect, the NetSight Server must be restarted. To enable beta features:

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Advanced Suite Settings.

3. In the right-panel, select the **Enable All Beta Features** checkbox and enter the NetSight Beta Activation Key. Contact Extreme Networks Support to obtain a Beta Key.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.
5. For this setting to take effect, the NetSight Server must be restarted.

Alarm Configuration

Use the Alarm Configuration view to configure options for how alarms are handled on your network. These settings apply to all users.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Alarm Configuration. The Alarm Configuration view opens.
3. In the **Consolidated Email Option** section, the **Enable Email digest** option lets you combine alarm action emails into a single email. Select the option and specify an interval. Email notifications will be collected over the specified interval and then delivered as a single consolidated email.
4. In the **Alarm History** section, select the desired options:
   Enable Detailed Alarm History – By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared. If you enable Detailed Alarm History, repeat occurrences of an alarm being raised will also be recorded.
   Preserve Triggering Events in Alarm History – This option preserves alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by clicking the View Trigger button in the Alarm History window.
   Number of Days to Maintain Alarm History – Specify (in days) how long the Alarm History will be retained.
5. Select the **Enable Sender Overrides** option to add an E-Mail Sender and E-Mail Sender Password field to the Console Alarms Manager Edit Action Overrides window. This allow you to override the sender of an email for an alarm email action, including the ability to set the sender's password, if needed. Since alarms are typically sent out as email/text messages, this option allows IT staff to set different ring-tones based on the alarm definition. Doing this on a smartphone typically involves changing the ring-tone for calls from a specific person.

6. Use the **Alarm Action Defaults** section to define the default content contained in alarm action messages. For example, with an email action, you can define the information contained in the email subject line and body. With a syslog or trap action, you can specify certain information that you want contained in the syslog or trap message. These values will be used unless they are overridden in an individual alarm.
   The message content is configured as a template, with the content passed directly as typed, except for the variable information which is specified by $keyword. The variable information ($keyword) is replaced with information from the alarm when the alarm action is executed.
   For an explanation of each field, see the Alarm Configuration view.
   For a complete list of available Alarms Manager keywords, see the Edit Action Overrides window in the Console online Help.
7. Click the **Advanced Settings** button to open the Alarm Advanced Settings window where you can set advanced alarm options.
8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Alarm/Event Logs and Tables Options

Use the Alarm/Event Logs and Tables view to specify options for limiting disk usage by alarm and event logs and NetSight server logs. These settings apply to all users. You must be assigned the appropriate user capability to configure these options. For more information on configuring log files, see the NetSight Log Files Help topic in the Console online Help.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Event Logs. The Event Logs view opens.
3. In the **Number of Event Logs to limit** section, you can select an option to limit the number of application log files that are saved to the `<install directory>\NetSight\appdata\logs` directory. (The option does not limit the number of Traps or Syslog logs that are saved.) Select one of the following options:
   - **Do not limit the number of log files saved** -- Allows you to keep any number of application log files.

- **Limit the number of log files saved to** -- Sets a limit to the number of application log files saved. Older files are deleted when the maximum number is reached. Enter the desired number.

4. In the **Number of Server Logs to limit** section, you can select an option to limit the number of server log files that are saved to the `<install directory>\NetSight\appdata\logs` directory. Select one of the following options:
   - **Do not limit the number of log files saved** -- Allows you to keep all server log files.
   - **Limit the number of log files saved** -- Sets a limit to the number of server log files saved. Older files (determined by the date of the file in the filename) are deleted when the maximum number is reached. Enter the desired number.
5. In the **Number of Rows to keep in Event and Alarm tables** section, specify settings that determine the number of rows that will be maintained in all of the tables in the Alarm and Event Log view. The table size reaches an absolute limit when the number of rows is equal to the value of the two parameters added together minus one. With the next entry, the table is clipped back to the number of rows set by the **Clip to nnnn rows value**. Subsequent entries will allow it to grow again until the **Clip when above is exceeded by nnnn rows** limit is reached and the table is again clipped.
6. In the **Event Log entry timestamp format** section, specify the timestamp format used for event log entries in the actual application log files. (This option does not affect the log entries displayed in NetSight client Event Log views.) Select one of the following options:
   - **Use raw timestamp format** -- Displays timestamps in a raw non-readable format.
   - **Use ISO 8601 timestamp format** -- Displays log entry timestamps in a readable format that makes it easier to view the files in a text file.
7. In the **Event and Alarm Table Host/Port Names** section, you can configure host name and port name resolution, and display the device hostname in the Source column in alarm and event tables:
   - **Resolve source host names** - Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to enable/disable host name resolution for the Event and Alarm tables only. (Host name resolution is enabled globally using the Suite Name Resolution option.)

- **Display host name in source column if available**
- **Resolve port name/alias** - Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to enable/disable port name resolution for Event and Alarm tables only. (Port name resolution is enabled globally using the Suite Name Resolution option.)

8. The Execute Command Script feature includes script contents in logged events, which is not secure if the script includes passwords. If the **Execute Command Script** option is deselected (default), the script is removed from the logged event. Select this option to include script contents in Execute Command Script events.
9. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Client Connection Options

Use the Client Connections view to configure client connection options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Client Connections.
3. In the right panel, select the **Enable disconnect from user inactivity** checkbox if desired, and specify the amount of time (in minutes) before the disconnect will take place. This option specifies a duration of end user inactivity (no keyboard or mouse activity) before the user will be disconnected from the NetSight Server. If this option is enabled, after the specified amount of time, the end user will be disconnected from the NetSight Server and the application will close. This option will apply to the current logged-in user. You must be a member of an authorization group that has been assigned the Server Information > Disconnect Clients capability to configure this option.
4. Select the **Redirect Client/Server SNMP Communications** checkbox, if desired. When a client and server are running on different workstations, SNMP requests are made from the client workstation and device status polling requests are made from the server. Checking this option redirects all SNMP requests through the server. In this configuration, the server uses the same Status Polling settings that would have been used by the client. Redirecting all SNMP requests to the server workstation could adversely affect performance of NetSight applications. This option applies to the current logged-in user and has no effect when the client and server are running on

the same workstation. You must be a member of an authorization group that allows users to configure SNMP Redirection in order to configure this option.

5. Configure the **Messaging Credentials** option. Messaging credentials are used for establishing connections between the NetSight server and Extreme Access Control engines and the Extreme Management Center server. If your network includes Extreme Access Control engines running version 4.0.1 or earlier, you must enable the "Allow legacy credentials for messaging connections" checkbox. If your engines are version 4.1 or later, you should disable the checkbox. This option applies to all users.
6. Select the **Show Credentials** checkbox to view the current messaging credentials. This option applies to all users.
7. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Scheduling a Database Backup

Use the Database Backup view to schedule backups of the NetSight database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all NetSight applications is saved and readily available, if needed. These option applies to all users.

Select one or more days of the week and specify a time for the backup to be performed. The backup will take place at the same time for each selected day.

The database is backed up to the specified directory. Saving backups to a separate location such as a network share ensures that an up-to-date copy of the database is available should a problem such as a server disk failure occur. The backup directory must exist and be writable or it will not be accepted.

Both the start and stop of the database backup are logged to the Console Event View log for verification and tracking purposes.

For more information, see Tuning Database Backup Storage in Performance Tuning section of the NetSight Technical Reference.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Database Backup.
3. In the right panel, select the days of the week and a time for the backup to be performed.

4. Specify whether to save all backup files or limit the number of files saved. If you specify a number of files to save, then older backups are removed after a scheduled backup is completed and the limit has been reached.
5. Specify the directory where the backup will be stored.
6. The **Backup Alarm and Reporting Database** checkbox lets you enable and disable the automatic backup of alarm data and OneView reporting data. Because the alarm and reporting databases can be quite large, this allows you to control the amount of disk space used by the database backup operation.
7. You can customize the date and time formats of backup files by selecting the option that formats the date – day (DD), month (MM), and year (YYYY) – according to your personal preference.
8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Data Display Format Options

Use the Data Display Format view to specify your network mask, MAC address separator, how to display end-system MAC addresses in right-panel tables, and auto group delimiter display options. You can also specify how to display devices in the device tree. These settings will apply to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Data Display. The right-panel Data Display view is displayed.
3. Specify one of the following network mask options:
   - **CIDR (where translation is possible)** – Network masks are entered and displayed using CIDR (Classless Inter-Domain Routing) format. CIDR format uses a slash followed by a number between 8 and 32, to define the number of contiguous, left-most "one" bits that define the network mask. For example, */16* for a 16-bit mask.

     NOTE: Dot delimited masks without contiguous left-most "one" bits cannot be translated to CIDR. For example, the dot-delimited mask *255.0.255.0* is a valid mask, but cannot be displayed in CIDR format.

- **Dot Delimited** – Network masks are entered and displayed using dotted decimal format. Dotted decimal notation represents IP addresses and network masks as four octets separated by periods. For example, a 16-bit mask in dotted decimal notation is *255.255.0.0*.

4. Specify whether you want MAC addresses displayed with a period (.), colon (:), or dash (-) separator (e.g. 00.00.1D.76.66.66, 00:00:1D:76:66:66, or 00-00-1D-76-66-66).
5. Specify how you want to display end-system MAC addresses in right-panel tables. You can display them as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix. This allows you to display the associated vendor the MAC address belongs to, if an OUI mapping exists. You can also limit the vendor name to a certain number of characters, if desired. When the **Display Unknown MACs as Unknown** checkbox is selected, the MAC address for unknown users is displayed as "Unknown" in the End-Systems view. If the checkbox is not selected, the pseudo MAC address assigned to each device is displayed instead of "Unknown" for end-systems learned on an L3 controller.
6. Specify the Auto Group Delimiter you want to use. This character is used to separate the values that define a device's **Contact** and **Location** grouping in the left-panel device tree. Sub-groups in the **Grouped By** > **Contact** and **Grouped By** > **Location** folders are automatically created based on the Contact and Location values in the Console Properties Tab (Device). This option defines the delimiter that is used to separate those values into groups. For example, using the default delimiter (/), a device's location defined as *NewHampshire/Salem/Closet3* will automatically create a hierarchy of three sub-groups under the **Grouped By > Location** folder.
7. Specify how device names should be displayed in the left-panel tree:
    - **Use IP Address** – use the device's IP address.
    - **Use System Name** – use the administratively-assigned name of the device taken from the *sysName* MIB object.
    - **Use User Defined Nickname** – use the user-defined nickname as defined in the Console Properties Tab (Device).
8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Date/Time Format Options

Use the Date/Time Format view to customize the date and time formats to your own personal preference. These settings will apply to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Date/Time Format in the left-panel tree. The right-panel Date/Time Format view is displayed.
3. Select the **Date** option that formats the date – day (DD), month (MM), and year (YYYY) – according to your personal preference.
4. Select the **Time** option that formats the time – 12-hour or 24-hour clock – according to your personal preference.
5. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Diagnostic Configuration Options

Use the Diagnostic Configuration view to configure the level of information collected in client-side diagnostic logs. The information collected in these logs can be used for troubleshooting purposes. Each NetSight application has its own log. The diagnostic information is recorded in the log for the application you are currently working in. The logs are located in the following directory:
Windows: \Documents and Settings\<user home directory>\Application Data\NetSight\logs
Linux: ~/NetSight/logs

The table in this Options view lists the NetSight applications and various NetSight components, and lets you configure the level of information to be collected for each one.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Diagnostic Configuration in the left-panel tree. The right-panel Diagnostic Configuration view is displayed.
3. In the table, select the row(s) you would like to edit, and toggle the Show/Hide Table Editor button to display the Table Editor row at the bottom of the table. In the Table Editor row, click on the last column and use the drop-down list to select the

desired level:

- Restore Defaults – restores the level to its factory default setting.
- log4j File Override – sets the level to the level specified in the log4j.properties file.
- Off – turns off all diagnostic logging.
- Critical – records only Error events.
- Warning – records Warning and Error events.
- Informational – records Warning, Error, and Info events.
- Verbose – records debug information in addition to Warning, Error, and Info events.

CAUTION: The Informational and Verbose settings will create large log files and may impact system performance.

4. Once you have selected a new level, a green exclamation mark (!) marks the cells that have been changed (but not Applied) and the **Apply** button becomes active. Click **Apply** to apply the changes to the table.
5. Click **OK** to close the window.

Setting ExtremeNetworks.com Update Options

Use the ExtremeNetworks.com Update view to configure options for accessing the ExtremeNetworks.com website to obtain information about the latest NetSight product releases and Extreme Networks firmware releases available for download. These settings apply to all users. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to configure these options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select ExtremeNetworks.com Update. The ExtremeNetworks.com Update view opens.
3. To schedule a routine time to check for updates, use the drop-down list to select the desired frequency (**Daily**, **Weekly**, **Disabled**) for checking for updates. If you specify a Weekly check, use the drop-down list to select the day of the week you wish the

check to be performed, and set the desired time. If you specify a Daily update, set the desired time.

4. If necessary, you can change the NAC assessment web update server. This is the web update server used by NAC Manager to update NAC assessment server software. This update operation pertains only to Extreme Access Control on-board agent-less assessment servers.
5. If your network is protected by a firewall, you will need to configure proxy server settings to use when accessing the ExtremeNetworks.com website. In the HTTP Proxy Server section, click **Edit** to open the Edit Proxy Settings window. Select the **Specify Proxy Server** checkbox and enter your proxy server address and port ID. Consult your network administrator for this information. If your proxy server requires authentication, select the **Proxy Authentication** checkbox and enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server. Proxy credentials are cached once used successfully. If you change them here, it is recommended that you restart the NetSight Server to clear the old credentials from the cache. Click **OK**.

   NOTE: The update procedure will use these proxy settings only when necessary, otherwise the settings will be ignored.

6. Enter the credentials that will be used to access the ExtremeNetworks.com website to obtain firmware and NetSight update information. You will need to create an account at ExtremeNetworks.com and define a user name and password for the account, then enter the same credentials here.
7. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

MAC OUI Vendor List

Use the MAC OUI Vendor List view to display the IEEE OUI and Company_id Assignments public mapping list, and update and modify the list, if desired. For example, you can update the list to the latest version from the IEEE website, and if you have devices that do not have an OUI (Organizational Unique Identifier), you can add your own vendor entries.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder and select MAC OUI Vendor List. The MAC OUI Vendor List view opens.

3. Use the toolbar buttons at the top of the table to add, edit, or delete MAC OUI vendors, or update the MAC OUI Vendor list from either the IEEE website or a file.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Name Resolution Options

Use the Name Resolution view to set options related to host name and port name resolution.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Name Resolution. The Name Resolution view opens.
3. Use the Host Name Resolution section to set options for resolving host names to IP addresses and IP addresses to host names.
   a. The **Enable Name Resolution** option allows host names to be displayed in place of IP addresses throughout NetSight. When enabled, the feature is primarily used by NetFlow. With name resolution enabled, flow data would show "Client=rsmith-ws Server=proxy-usa", rather than "client=134.141.1.2 server = 134.141.1.1". The option is off by default because name resolution can add additional load on the network's DNS server.
   b. The **Use short hostnames for local addresses** option is enabled by default when hostname resolution is enabled, and applies to OneView only. When enabled, the hostname cache will remove the fully qualified hostname's domain if it matches one of the specified local address domains. For example, "jsmith-ws.mycompany.com" would display as "jsmith-ws" if mycompany.com is listed as a local address domain. This option can be disabled when troubleshooting problems with hostname resolution, or if IP addresses are preferred.
   c. The **Local Address domains** is a list of *home domains* that will be deleted from a local hostname when it is added to the hostname cache. Use the Add Domain field to add or remove a domain. You can add multiple home domains when subdomains are defined for your network. This option applies to OneView only.
      The first time the hostname cache service is started, if the Local address domains list has not been defined, NetSight will attempt to auto-populate it by resolving the IP address of the NetSight server. If it resolves to a subdomain,

NetSight will create multiple entries for all subdomains but the root domain (.com). If it cannot do this successfully, the list will not be populated.

d. Enter the **Maximum number of cached resolutions**, which is the maximum number of IP/hostname pairs that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

e. Enter the **Maximum number of pending resolutions**, which is the maximum number of hostname resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

f. The **Aging Threshold** option determines how long IP/hostname pairs will be cached in memory. After the aging threshold time has passed, the IP/hostname pair is removed from the cache in order to prevent stale IP-hostname associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, hostnames will continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

g. The **DNS Lookups Per Minute** option set the maximum number of hostname lookups that the DNS server can perform each minute. This prevents hostname resolution from using so many resources on a switch that switching of real traffic is affected.

4. Use the Port Name Resolution section to set options for resolving device port indices to port names and port aliases, and device port names and port aliases to port indices.

   a. Enter the **Maximum number of cached resolutions**, which is the maximum amount of port data that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

   b. Enter the **Maximum number of pending resolutions**, which is the maximum number of port name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

   c. Enter the **Interface name change polling interval**, which specifies how often the port name resolution service checks devices to see if port information has changed.

5. Use the **Advanced Settings** button to open the Name Resolution Advanced Settings Options window, where you can set advanced name resolution options.

6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

NetSight Feedback Program

This option allows you to enable or disable participation in the NetSight Customer Feedback Program. If you participate, NetSight gathers anonymous usage information that will be used to better understand how NetSight software is used and to make decisions on enhancing the product. This bi-directional communication with ExtremeNetworks.com also enables features for you such as the ability to get best practices firmware configurations, find the latest firmware updates based on your own network, create Support cases directly from NetSight that automatically upload troubleshooting information, and more.

The information gathered will not be used for marketing purposes or to contact you.

Setting NetSight Server Health Options

Use the NetSight Server Health view to select an option to send an email if the NetSight database goes down, and when the database comes back up.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select NetSight Server Health. The NetSight Server Health view opens.
3. Select the **Send email** option.
4. Enter the email address of the person who should receive the notification.
5. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Network Monitor Cache Options

The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from multiple places including slot and port details (Entity, ifTable), default role (Policy), neighbor link details (CDP, EDP, LLDP), Ethernet Automatic Protection Switching (EAPS), and Multi System Link Aggregation (MLAG).

The cache is maintained in a two-tiered structure: device physical data is cached to the database and a fast in-memory cache maintains a subset of this data in memory on the server. The in-memory cache can contain all or a subset of devices stored in the database.

On the specified polling interval, the data is validated and automatically updated as necessary. Decreasing the poll interval will increase background SNMP performed by the server.

Storing this information greatly improves performance for views in NetSight that request it. The cache should generally be left enabled for the best experience.

Use the Network Monitor Cache view to configure options for the cache.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Network Monitor Cache in the left-panel tree. The right-panel Network Monitor Cache view is displayed.
3. Use the **Enable Device Cache** checkbox to enable or disable the Network Monitor Cache. Enabling the cache improves performance for NetSight views that request this information.
4. Use the **Enable In-Memory Caching** checkbox to enable or disable the in-memory cache. To limit memory usage, you can disable the In-Memory Cache and have the network monitor cache rely directly on the database.
5. Use the **Maximum In-Memory Cache Size** option to set the maximum number of devices whose data will be stored in the In-Memory Cache. This option lets you adjust the amount of memory the cache will use.
6. Use the **Data Polling Interval** option to set the frequency (in minutes) that the device data is checked for changes. If the device data is stale, the data is refreshed in the cache. Reducing the interval will increase background SNMP performed by the server.
7. Use the **Advanced Settings** button to open a window where you can set network monitor cache advanced options.
    - **Maximum number of SNMP worker threads** option. The cache is populated with results from SNMP queries to devices. If multiple devices are added to the cache at the same time, this number determines the maximum number of threads that can send SNMP queries in parallel.

- **Per-Feature polling overrides.** Allows you to set unique polling intervals for individual cache features that should be polled more frequently. Set to 0 to use the interval set for the Data Polling Interval.

Setting Port Monitor Options

Use the Port Monitor view to specify Port Monitor display options. These settings will apply to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder and select Port Monitor. The Port Monitor view opens.
3. In the **Interval between Polls** field, enter the amount of time (in seconds) that should elapse between polls of the device.
4. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
5. In the **Enable Display of Port Monitor Data** section, use the checkboxes to specify what data will be displayed for a Port Monitor session. If the Show Empty Panels Collapsed checkbox is selected, panels without information will be collapsed so those panels with information are easier to view.
6. In the **Maximum Open Port Monitor Count** field, specify the maximum number of Port Monitor windows that can be open at one time. If too many windows are open at one time, system operation may be impacted. The default setting is 5.
7. Click **OK** to set the option and close the window.

Setting Services for NetSight Server Options

Use the Services for NetSight Server view to specify your TFTP settings. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Services for NetSight Server.

3. Specify a TFTP root directory, whether you are using the NetSight TFTP server or another TFTP server. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to create files to or read files from this directory and any of its subdirectories. Use the default root directory, or if you would like to use an alternate root directory, enter a path to that directory in this field or use the **Browse** button to navigate to the directory. Changing the TFTP root directory may require restarting the TFTP server.

NOTE: If you are using a TFTP server other than the NetSight TFTP service, keep in mind the following requirements when setting the path to your root directory:

- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.
- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive (e.g. C:\ or D:\).
- If you are using a TFTP server on a remote system, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (UNIX or Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the tftpboot directory on the remote drive)
  use
  `\\yourservername\tftpboot\`

4. If the TFTP server resides on a remote system, or if the local system is configured with multiple IP addresses, enter the IP address for the TFTP service in the **TFTP Server IP Address** field. This field accepts both IPv4 and IPv6 addresses.
5. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting SMTP E-Mail Server Options

Use the SMTP E-Mail Server view to specify the SMTP E-Mail server that will be used by the NetSight E-Mail notification feature. The E-Mail notification feature is used in Console's alarm action configuration, as well as in Inventory Manager's Capacity Planning report scheduling and in Automated Security Manager actions. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select SMTP E-Mail Server.
3. In the right panel, specify the SMTP (E-Mail) server that should be used for outgoing messages generated by the E-Mail notification feature.
4. Enter the sender's address that will be inserted in outgoing e-mail notification messages. The address should be in a fully qualified format such as "sender's name@sender's domain."
5. Enter the password that will be provided by the user before the email can be processed.
6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Status Polling Options

Use the Status Polling view to specify options for polling devices in the left-panel device tree. Console uses the polling options and poll groups defined here to contact the devices and update tree information. When a device is added to the NetSight database using the Add Device menu option or a Console CDP Seed IP Discover, it is added to the default poll group selected here. (A Console IP Range Discover lets you assign devices to any of the three poll groups.) You can then reassign individual devices or device groups to a different poll group using the Access view in the Console Properties tab. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Optimal Poll Intervals

There are three distinct poll groups, and each device belongs to one of the three groups. This lets you poll critical devices at a more frequent interval, while polling non-essential devices less frequently.

The overall density of polling is controlled by the **Maximum number of devices to contact at once** setting. This determines the maximum number of devices from each group that can be polled at any given time. Console always attempts to poll up to the maximum number of devices until all of the devices in the three groups have been polled. As responses are received and devices are removed from the poll queue, other devices are added to the queue. Once all the devices have been polled, Console stops polling and batches information to update clients.

If the Maximum number of devices to contact at once is too high, such that the poll density is too high, system performance will degrade quickly. The optimal poll setting is dependent on many factors including but not limited to CPU speed, RAM, and network devices. As the number of devices that you are polling increases, the poll density (Maximum number of devices to contact at once) should be reduced to increase performance.

The default Maximum number of devices to contact at once setting and poll group intervals provided as defaults are a good starting point. If necessary, adjust the values to optimize status polling for your network.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Status Polling. The Status Polling view opens.
3. In the SNMP section, set the status polling options for devices whose poll type is set to "SNMP."
   a. Set the **Maximum number of devices to contact at once**. This is the maximum number of IP addresses that Console will attempt to contact simultaneously.
4. In the Ping section, set the status polling options for devices whose poll type is set to "Ping."
   a. Set the **Number of Ping Retries**. This is the number of attempts that will be made to ping a device. The default setting is 3 retries, which means that Console retries a timed-out request three times, making a total of four attempts to contact a device.
   b. In the **Length of Ping Timeout field**, enter the amount of time (in seconds) that Console waits before re-trying to contact a device. The default setting is 3 seconds. The maximum setting is 20 seconds.

   NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

   c. Set the **Maximum number of devices to contact at once**. This is the maximum number of IP addresses that Console will attempt to contact simultaneously.

5. In the Poll Group section, there are three poll groups that each define a unique poll frequency. A poll frequency specifies the actual length of the poll cycle. You can rename the poll groups according to your network's needs and specify different poll frequencies. For example, if you are monitoring devices on the other side of a WAN link, you can rename a poll group to "WAN Devices" and then assign that poll group to those devices. Poll group names must be unique. For more information on setting poll group intervals, see the guidelines outlined in Optimal Poll Intervals.
6. Select one group as the default poll group. When a device is added to the NetSight database using the Add Device menu option or a CDP Seed IP Discover, it is added to the default poll group selected here. (IP Range Discover lets you assign devices to any of the three poll groups.) You can also assign individual devices or device groups to a specific poll group using the Access view in Console's Properties tab.
7. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting System Browser

Use the System Browser view to specify the web browser for NetSight to use when launching web pages from NetSight applications. This setting applies to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select System Browser.
3. In the right panel, select your preferred web browser. The browser selections displayed depend on the web browsers installed on your system. Select Default to specify the system default browser.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Tree

Use the Tree view to specify whether a warning message will be displayed when performing drag and drop operations on devices and device groups in the network elements tree. For example, if you drag a device in the tree to a user-defined folder, the warning appears asking if you are sure you want to drop the selected device into this folder. This warning allows you to verify that you do indeed want to perform a drag and drop operation to that folder, and prevents you from inadvertently moving devices. However, if you find it annoying to have the warning appear each time you do a drag and drop operation, you can deselect the option. This setting applies to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Tree.
3. In the right panel, deselect the checkbox if you do not want the warning to appear.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Web Server

Use the Web Server view to specify the HTTP and HTTPS port ID for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch NetSight client applications. By default, NetSight uses port ID 8080 (HTTP) and 8443 (HTTPS). If you change the port ID, you must restart the NetSight Server for the change to take effect.

This setting applies to all users. You must be assigned the appropriate user capability to change this setting.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Web Server.
3. In the right panel, enter the desired port IDs.
4. Specify a session timeout value for all NetSight web-based views, such as NetSight OneView web pages and Console FlexViews.
5. The Password AutoComplete option lets you disable automatic password completion for users logging into NetSight web interfaces such as OneView. Note that for Extreme Access Control web interfaces, you must enforce from the **Extreme Access Control** tab for the option to take effect.
6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.
7. You must restart the Extreme Management Center Server for any Port ID changes to take effect.

Related Information

For information on related windows:

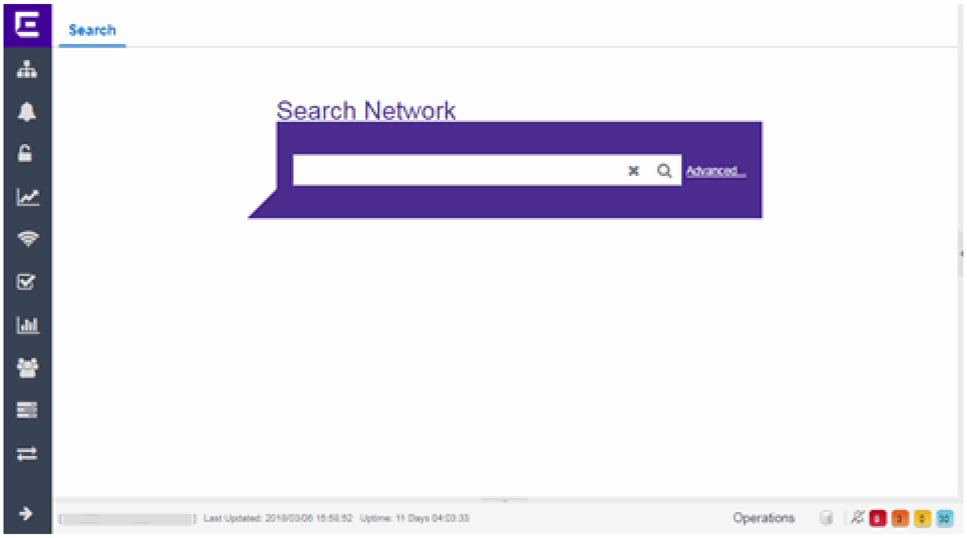
- Suite Options Window

Search Network

Extreme Management Center's Search Network is a powerful diagnostic tool for locating a network device or end-system you wish to troubleshoot by allowing you to display it in PortView. You can search by MAC address, IP address, or AP serial number, as well as Extreme Access Control end-system name, username, and registration custom field attributes. A device must be in the Extreme Management Center database, or it must be a client of a device in the database, for the search to function. For a client device, either statistics collection must be enabled for the device, or the client must be an Extreme Access Control authenticated client.

In addition, there are two Advanced Search options, accessed from the Advanced link to the right of the **Search Network** field: searching in Compass and searching in Maps.

To view Extreme Management Center Search Network, you must be a member of an authorization group assigned the NetSight OneView > Access OneView Search capability. To perform a Search with Compass, you must also have the NetSight Console > Launch a NetSight Console Client capability. (For more information on authorization capabilities, see the Help topic, "How to Configure User Access to Extreme Management Center Applications," located in Suite-Wide Tools > Authorization Device Access.)



This Help topic provides information on the following topics:

Using Extreme Management Center Search Network

In the **Search Network** field, enter a MAC address or IP address and press **Enter** to begin the search. You can copy the IP or MAC address from another source and enter it into the **Search Network** field. You can also search on AP serial numbers, and by Extreme Access Control end-system hostname, user name, and registration custom field attributes.

Depending on the type of item you searched for, the secondary navigation bar displays one or more **PortView** tabs, with information pertaining to your search item.

The **Overview** tab always displays, which provides a topological display of device relationships. You can right-click on the devices in the topology to launch additional reports for the device. For more information see the PortView Help topic.

Search Examples

Following are some examples of different kinds of searches you can perform using the Extreme Management Center Search Network.

Search your Network for an End-System MAC Address

You can search on an end-system's MAC address. For example, you can copy an end-system's MAC address listed in the **Control** tab's End-System view and paste the MAC address into the **Search Network** field.

Search your Network for an Extreme Access Control Authenticated Client IP Address

You can also search on an Extreme Access Control authenticated end-system's IP address. For example, you can copy an end-system's IP address from the **Control** tab's End-Systems view and paste it into the **Search Network** field.

Search your Network for a Device IP Address

To perform a search on a device, you can copy a device IP address from the **Network** tab. The search results show only the single device. Right-click on the device to open additional reports.

Search Options/Limitations

The maximum number of PortView Search results displayed at one time is configured in the Management Center Options (Administration > Options > Management Center > Session Limits). The default maximum number is five. Once the limit is reached, a dialog displays, indicating the limit is reached and the existing view must be closed.

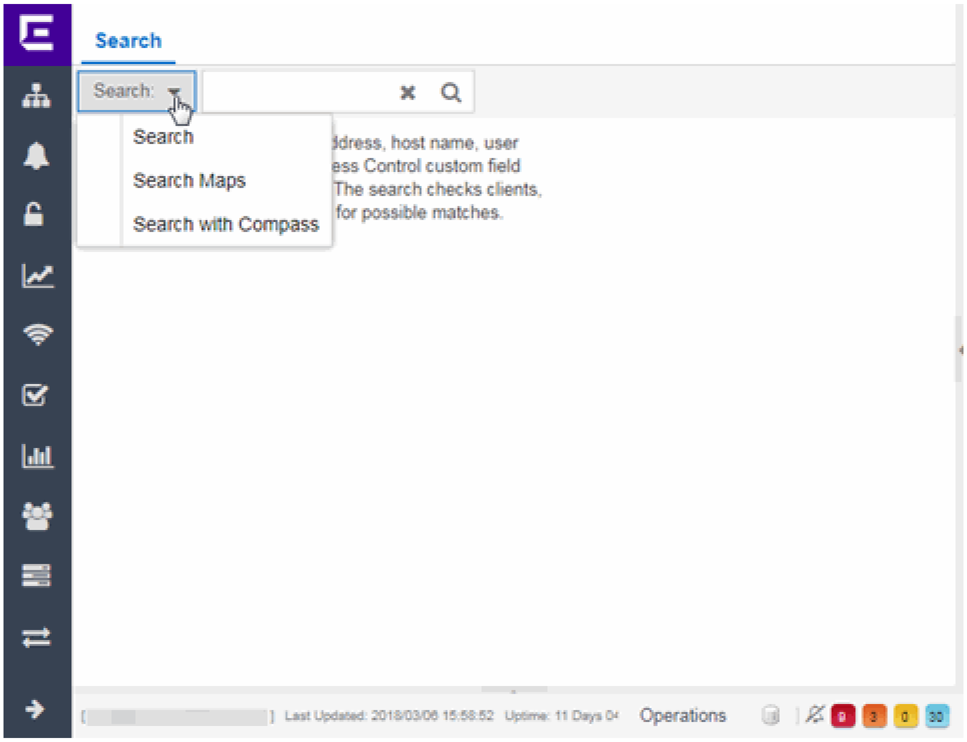
In the **Overview** (search results) tab, the device topology is displayed showing the relationships between a specific set of devices: Wireless Controller, Identity and Access Gateway, AP, switch, and client. The greatest number of devices displayed is five devices for a wireless client in an Extreme Access Control authenticated environment (six devices may be returned if the client is also connected via wire). The number of devices returned becomes smaller as you search for one of the five devices. For example, if you search for an AP instead of a client, four devices are returned. If you search for a Wireless Controller, Extreme Access Control Gateway, or switch, one device is returned.

Advanced Search Options

The Advanced Search, accessed from the Advanced link to the right of the **Search Network** field, provides two additional search options available from the **Search** drop-down menu at the top-left of the Search page.

- **Search in Maps** — Allows you to search your existing maps to find a wired or wireless client or device. If the search item is found, the map opens on a separate tab. For more information, see Maps Overview.

- **Search with Compass** — Provides additional fields, allowing you to refine your search. For more information, see Search with Compass.



ddress, host name, user
ess Control custom field
The search checks clients,
for possible matches.

Search with Compass

The Search with Compass option provides a variety of search filters, allowing you to narrow your search parameters. Compass is a powerful search tool that provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations.

You can access the Search with Compass option from the **Search** drop-down menu at the top-left of the Search page. To perform a search, specify the following information:

- Device Group (Search Scope) — Use the drop-down menu to select a device group to search. The menu is populated with the system and user-defined device groups in Console. If you do a search on a user-defined device group that contains interfaces, the whole device on which the interface is located is searched.

- Search Type — There are multiple search types available from the drop-down menu. See the following section for a description of each type.
- Address (Search Parameters) — If you provide specific search parameters (such as an IP address or MAC address), Compass returns information on those parameters if it finds them within the selected device group. If you do not provide specific search parameters, Compass returns information on everything within the device group.

When the search is complete, the results display in table form. You can manipulate table data in several ways to customize the view for your own needs:

- Click on the column headings to perform an ascending or descending sort on the column data.
- Use the column heading drop-down arrow to select the Columns option and hide or display different columns in the table.
- Use the column heading drop-down arrow to filter, sort, and search the data in each column in the table.

You can define the search options the Compass Search uses on the **Administration** > **Options** tab (Administration > Options > Compass). These options determine the data sources used with Compass searches. In addition to search options, you can also configure search limit settings, which help limit the Extreme Management Center server resources used for the searches.

Compass Search Types

The following Compass Search types are available.

- Auto — The Auto search auto-detects the address format you enter in the **Address** field, and performs the appropriate search. Enter the full IP, MAC, or username in the **Address** field and select a device group as a search scope.
- All — The All search finds any network element aware of the devices within the selected scope, and lists the addresses with which they are associated. Data is collected from all the MIBs that Compass implemented. The All search ignores any search parameters entered in the **Address** field.
- MAC Address — The MAC Address search finds any device aware of the specified MAC address within the selected scope and lists the addresses associated with it.
- IP Address — The IP Address search finds any device aware of the specified IP address/hostname within the selected scope and lists the addresses with which it is associated.

- IP Subnet — The IP Subnet search finds any device aware of the specified IP subnet within the selected scope and lists the end stations in the IP subnet. The address must contain both an address and mask separated by "/".
- User Name — The User Name search finds any device aware of the specified user name within the selected scope and lists the addresses with which it is associated.
- Multicast Address — The Multicast Address search finds any device aware of the specified multicast address within the selected scope and lists the addresses with which it is associated.

Related Information

For information on related tabs:

- Administration
- Alarms and Events
- Network
- Reports
- Wireless

Extreme Management Center Compass SNMP MIBs Descriptions

This topic provides a brief description of the MIBs and Tables that can be chosen as Compass Search Options when setting Compass options.

ipNetToMedia

IP Address Translation table used for mapping from IP addresses to physical addresses. This table is read whenever an entry is found by IP Route or IP CIDR Route searches, regardless whether the IPNetToMedia is checked. Checking the IPNetToMedia checkbox only affects whether or not the entire IPNetToMedia table is read.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

802.1x Authentication (PAE)

Port Access Entity module for managing IEEE 802.1X.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

MAC Locking

Provides configuration and status objects pertaining to per port MAC Locking.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Enterasys IGMP

Extends the Standard IGMP MIB for configuration of IGMP on Enterasys devices.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Dot1dTpFdb

This table contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

Check this MIB to resolve MAC addresses to a port.

Enterasys 802.1x Ext.

Supplements/used in connection with the standard IEEE 802.1x MIB. It provides a convenient way to retrieve authentication status for Supplicants living on shared-media ports that use station-based access control. (Here, a MAC address is a much more natural table index than a port or interface number.)

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Node/Alias (ctAlias)

This MIB defines objects that can be used to discover end systems per port, and to map end system addresses to the layer 2 address of the port.

Check this MIB to resolve IP addresses to MAC addresses when the devices in your network support the Node/Alias (ctAlias) MIB.

IGMP Standard

MIB module for IGMP Management, it contains an IGMP Interface Table, having one row for each interface on which IGMP is enabled, and an IGMP Cache Table with one row for each IP multicast group for which there are members on a particular interface.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

IP Route

An entity's IP Routing table. This selection provides the ability to resolve IP addresses to MAC addresses.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

Dot1qTpFdb

A table that contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

PWA (Enterasys Port Web Authentication)

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

MAC Authentication

Used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

IP CIDR Route

The IP CIDR Route Table obsoletes and replaces the ipRoute Table current in MIB-I and MIB-II and the IP Forwarding Table. It adds knowledge of the autonomous system of the next hop, multiple next hops, and policy routing, and Classless Inter-Domain Routing.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

Dot1q VLAN Static

A table containing static configuration information for each VLAN configured into the device by (local or network) management. All entries are permanent and are restored after restarting the device.

Dot1q VLAN Current

A table containing current configuration information for each VLAN currently configured into the device by (local or network) management, or dynamically created as a result of GVRP requests received.

Enterasys Multiple Authentication

This MIB is used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication. Check this MIB to find ports that allow authentication of multiple users on a port.

Enterasys Convergence End Point

This MIB contains information about devices that support End Point Convergence. Check this MIB to find IP addresses running applications (e.g. Voice over IP) using Endpoint Convergence.

How to Discover Devices

Extreme Management Center allows you to discover the devices of your network and add them to the Extreme Management Center database.

NOTE: Before discovering devices, create the maps to which they belong. For additional information on creating maps, see How to Create and Edit Maps.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

You can discover new devices based on the following criteria:

- Seed addresses for CDP, LLDP, or EDP-compliant devices
- IP/Subnet masks
- IP Address Range

Discover automatically explores the defined network segment and creates a list of discovered devices. You can then save the discovered devices to the Extreme Management Center database, where they are displayed in the left-panel tree on the **Network** > Devices tab.

To discover devices, begin by using the **Site** tab to configure the default settings that apply to devices you add to Extreme Management Center and then configure individual devices and add them to the Extreme Management Center database via the **Discovered** tab.

NOTE: ZTP+ enabled devices use a different device discovery process. For additional information on discovering devices using ZTP+, see ZTP+ Device Configuration in Extreme Management Center.

Discovering Devices

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down menu.
3. Select the site from the left panel to which you are adding the devices.
4. Select the **Site** tab in the right-panel.

5. Select the **Discover** tab.
6. Click the **Add** button in the Addresses list to open the Add Address window.
7. Select **Subnet**, **Seed Address**, or **Address Range** in the **Discover Type** drop-down menu.
8. Enter the **Subnet**, **Seed Address**, or **Start Address** and **End Address**, depending on the **Discover Type** you select.
   - **Subnet** — Enter the IP address and subnet in the following format: *IP Address/Subnet Mask*
     - The *IP Address* must be one of the hosts in the subnet.
     - A **/** is required between the IP Address and Subnet Mask.
     - The *Subnet Mask* must use CIDR or dotted decimal notation.

     NOTE: When using dotted decimal notation, the network bits must be contiguous ones and the host bits must be contiguous zeros.

   - **Seed Address** — Enter the seed address for CDP, LLDP, or EDP-compliant devices.
   - **Address Range** — Enter the **Start Address** and **End Address** for the IP addresses in the same address range.

   NOTE: Extreme Management Center only allows a subnet search of a 16-bit mask or higher when discovering devices.

9. Click the **Add** button in the Profiles section of the window to open the Add Profile window. Select **New** in the drop-down menu to create SNMP and CLI credentials for the profile and click the **Save** button.

   Profiles allow you to configure different sets of SNMP and CLI credentials for read access, write access, and maximum access. Once you create profiles, assign them to devices to allow users appropriate access based on the credentials they use for a device.
10. Select the profiles you want the devices on your network to **Accept** or **Reject** using the **Profiles** list.
    For additional information about profiles, see [Profiles tab](#).
11. Select the **Automatically Add Devices** checkbox and any other appropriate actions for your devices in the Device Actions section of the window.

12. Repeat the process for all devices added to this site.
For additional information about sites, see Site tab.

13. Click **Save**.

14. Click **Discover**.

15. Open the Operations table at the bottom of the Extreme Management Center window by clicking the **Operations** button in the Bottom menu to monitor the progress of the device discovery.

16. Open the **Network** > **Discovered** tab when the device discovery is complete.
The **Discovered** tab displays.

Adding Devices

1. Open the **Network** > **Discovered** tab in Extreme Management Center.
For more information about the **Discovered** tab, see Discovered tab.

2. Select the devices you want to add to the Extreme Management Center database and click the **Add Devices** button. The Add Devices window opens.
The window is populated with the information you entered on the **Site** tab.

3. Enter any device-specific information, or change information that does not match the device defaults set on the **Site** tab.

4. Click the **Add** button.
The devices are added to the Extreme Management Center database and move from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

Related Information

For information on related topics:

- Sites
- Discovered
- How to Create and Edit Maps
- Device Operations

How to Add Users

Users are given access to parts of Extreme Management Center based on the authorization group to which they are assigned. Assign a set of capabilities for each authorization group and then add users to each authorization group depending on the capabilities they require.

NOTE: This topic assumes devices are already added to the Extreme Management Center database. For additional information on discovering and adding devices, see How to Discover Devices in Extreme Management Center.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

When you first log into Extreme Management Center the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to Extreme Management Center, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: Extreme Management Center does not save passwords. Users you create are authenticated against the Operating System, the RADIUS server, or the LDAP server, depending on the authentication method you select.

Create Authorization Groups

First, create authorization groups for each group of Extreme Management Center users.

1. Access the **Administration** > Users tab.
2. Click the **Acquire Lock** button in the Users/Groups Access section at the top of the tab.
   This button locks access to the tab for all other users and allows you to make changes to the authorization groups and authorized users.

3. Click the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using Extreme Management Center.
   The Capability section of the window allows you to expand each capability tree by selecting the arrow to the left of the checkbox to display more specific tasks. Select only those that apply to each user group. Additionally, you can search for a specific capability in the **Search** field above the tree.
5. Click the **Save** button to create the authorization group.
6. Repeat the process to create the necessary authorization groups.

Add Users to Authorization Groups

Next, use of the **Administration** > **Users** tab to create the users who require access to Extreme Management Center and add them to an authorization group depending on the level of access they require.

1. Click the **Add** button in the Authorized Users section.
2. Enter a User Name, a Domain/Host Name (if necessary), and select the Authorization Group with the appropriate level of access for the user.
3. Click the **Save** button to save the new user.
4. Repeat the process to add all Extreme Management Center users for each authorization group.

Select the Authentication Method

Finally, use **Administration** > **Users** tab to select the method by which users authenticate when accessing Extreme Management Center.

Extreme Management Center supports three authentication methods to authenticate users: using the underlying host operating system, using a specified LDAP configuration, or using specified RADIUS servers.

1. Select the **Authentication Type** using the drop-down menu in the Authentication Method section.
   The options change based on the **Authentication Type** selected.
2. Select the supplemental information based on the type selected.
3. Click the **Release Lock** button to allow other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

Related Information

For information on related topics:

- Users
- Authorization Group Capabilities

Compare Device Configurations

You can compare archived device configurations in Extreme Management Center by using either the **Network** > **Devices** tab or the Archive Details Report available in the **Network** > **Reports** tab.

In order to perform the compare configuration operation, you must be a member of an authorization group with the Inventory Manager > Configuration Archive Management > View/Compare Configurations capability.

This Help topic provides the following information:

- Selecting the Files to Compare
- Comparing the Files

Selecting the Files to Compare

Select the files to compare using either the **Network** tab or the **Reports** tab.

From the Network tab:

Use the **Network** tab to compare the last two archived configuration files for a device.

Select a device in the table and use either the **Menu** icon (≡) or the right-click menu off the device to select Configuration/Firmware > Compare Last Configurations.

From the Reports tab:

Use the **Reports** tab to compare two configuration files selected from all archived files for the device.

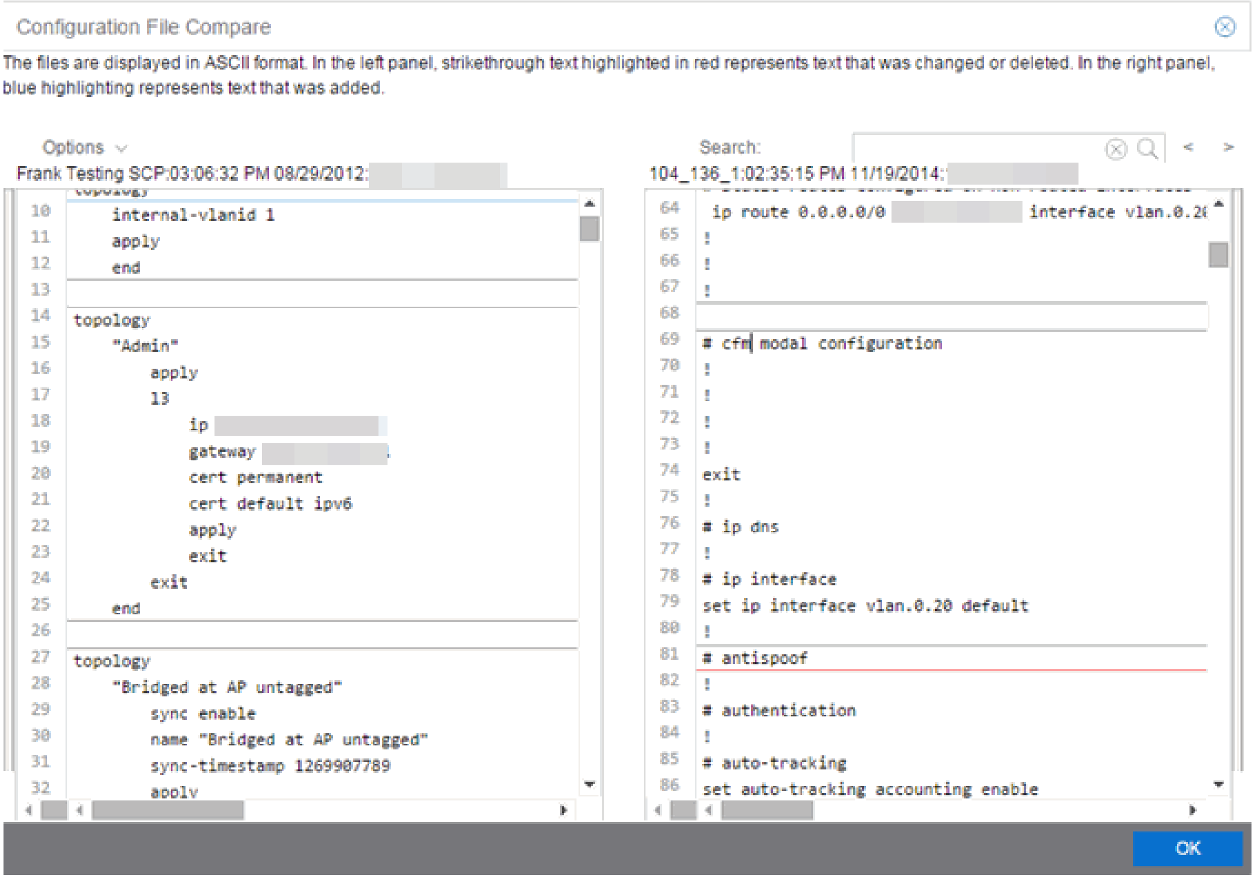
Select the Device > Device Archives report. Click on the **Archive Details** tab in the right panel and then click on the **Archives by Device** sub-tab.

The tab displays all the Extreme Management Center archives by device IP address. Select two files to compare and click **Compare Configuration**.

Comparing the Files

The Configuration File Compare window displays the files in two panels. Titles over each file show the archive name that contains the configuration file, the date, and the IP address of the device from which you create the configuration file.

Scroll through the two files to view file differences. Typically, the newer file displays in the right panel. You can use the "Swap sides" option to swap the files. In the left panel, strikethrough text highlighted in red represents text that is changed or deleted. In the right panel, blue highlighting represents text that is added.


Configuration File Compare

The files are displayed in ASCII format. In the left panel, strikethrough text highlighted in red represents text that was changed or deleted. In the right panel, blue highlighting represents text that was added.

Frank Testing SCP:03:06:32 PM 08/29/2012:[redacted]

```
    internal-vlanid 1
    apply
    end

topology
    "Admin"
        apply
        l3
            ip [redacted]
            gateway [redacted]
            cert permanent
            cert default ipv6
            apply
            exit
        exit
    end

topology
    "Bridged at AP untagged"
        sync enable
        name "Bridged at AP untagged"
        sync-timestamp 1269907789
        apply
```

104_136_1:02:35:15 PM 11/19/2014:[redacted]

```
 ip route 0.0.0.0/0 [redacted] interface vlan.0.2
!
!
!

# cfm modal configuration
!
!
!
!
exit
!
# ip dns
!
# ip interface
set ip interface vlan.0.20 default
!
# antispoof
!
# authentication
!
# auto-tracking
set auto-tracking accounting enable
```

Use the toolbar Options menu to control the look of the display window:

- Enable line numbers displays line numbers alongside the text.
- Wrap lines shows all the text in the column and removes the horizontal scroll bars.

- Enable side bars shows where the text differences are in the whole file.
- Swap sides swaps the files contained in the left and right panels.

TIP: Removing line numbers and side bars may speed up the display of larger files.

Use the **Search** field in the toolbar to perform a search in the panel side that is selected by the cursor. Use the forward and back arrows to search for the next or previous instance of the search term.

Related Information

For information on related topics:

- Network
- Reports

DeviceView

DeviceView is an Extreme Management Center component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and Extreme Management Center reports.

The primary launch point for DeviceView is from the **Network** tab. DeviceView can also be launched from other locations in Extreme Management Center and Console.

This Help topic provides the following DeviceView information:

- Requirements
  - Access Requirements
  - Data Collection Requirements
- DeviceView Reports
  - Left-Panel Device Summary
- Launching DeviceView

Requirements

Access Requirements

Access to DeviceView reports is determined by the user's membership in a Extreme Management Center authorization group and the group's assigned capabilities. The following list shows the capabilities required for full access to all the DeviceView reports.

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > FlexView > OneView FlexView Read Access

For more information on how to configure capabilities and authorization group membership, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

Data Collection Requirements

DeviceView reports require that historical data collection is enabled for the device. For information on configuring data collection, see Collect Device Statistics in the Devices section of the Extreme Management Center User Guide.

DeviceView Reports

The DeviceView is comprised of a left-panel device summary, and a selection of tabbed panels that display FlexViews and reports based on the device family.

The following table shows the reports available for EOS devices, ExtremeXOS devices, and wireless controllers. The reports displayed in a DeviceView vary according to the selected device.

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Ports***	Ports***	Ports***
User Sessions	User Sessions	User Sessions
Switch Resources	Device and Module Information	Controller History

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Power and Fan Status	Power and Fan Status	Active Access Points
Storage Utilization	Process Utilization	WLAN Services
CPU and Process Utilization	VLAN****	Active Clients
IP Traffic Summary	MLAG	Alarms and Events
Alarms and Events	VPLS	Archives
Archives	Port Utilization	
	Alarms and Events	
	Archives	

*Includes N-Series, S-Series, and K-Series devices.

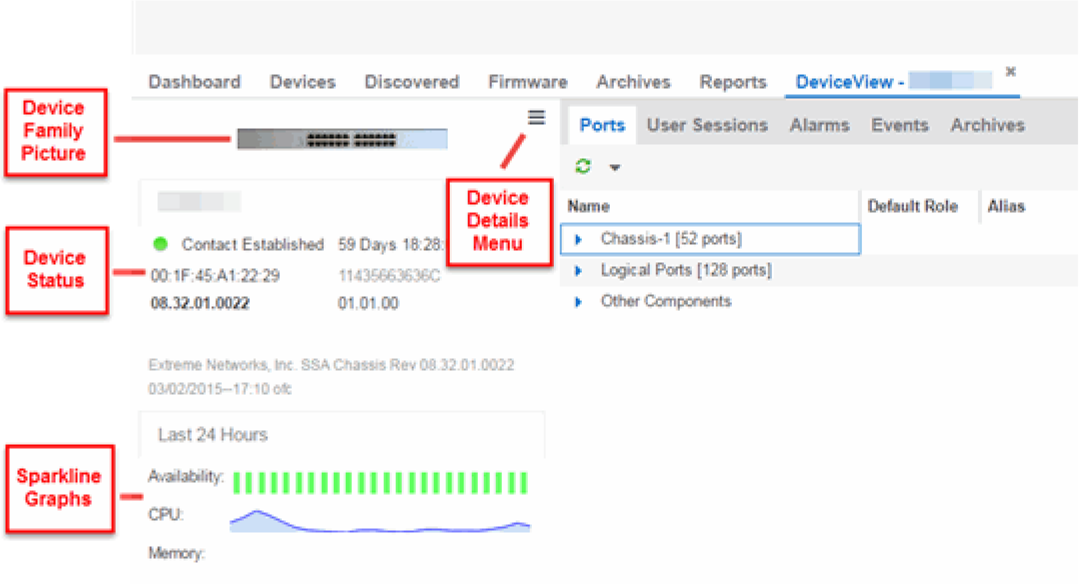
**Includes BlackDiamond, E4G, and Summit Series devices.

***Right-clicking ports and selecting Add to Device Group opens the Add to Device Group window, which allows you to select a device group to which to add the selected ports.

****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.



Contact Established 59 Days 18:28
00:1F:45:A1:22:29 11435663636C
08.32.01.0022 01.01.00

Extreme Networks, Inc. SSA Chassis Rev 08.32.01.0022
03/02/2015--17:10 ofc

Chassis-1 [52 ports]
Logical Ports [128 ports]
Other Components

Each device summary view includes:

- **Device Family Picture** — A generic device family picture for the device.
- **Device Status** — Indicates the alarm/device status for the device. The icon color indicates the severity of the most severe alarm on the device. A red icon indicates a critical alarm or the device is down. A green icon indicates that there are no alarms and the device is up.
- **Sparkline Graphs** — Provides network trends in dense, succinct charts that present report data in an easy to read, condensed format. You must have Historical Statistic Collection enabled in order to see the Sparkline graphs and other report data. If Historical Statistic Collection is not enabled, you will see a line that says, "Historical Statistic Collection Disabled." For information on configuring data collection, see Collect Device Statistics in the Devices section of the Extreme Management Center User Guide.
- **Firmware Updates Available** — If there are new firmware releases available for the device (based on the results from the latest Check for Firmware Updates operation), the Firmware Update icon displays. Right-click on the icon to open a window listing the current available firmware releases with links to download the firmware.
- **Device Details Menu** — Click the **Menu** icon (☰) in the upper right corner to access additional device reports.

Launching DeviceView

DeviceView can be launched from a variety of locations in Extreme Management Center.

Network Tab

The primary launch point for DeviceView is from the **Network** tab.

1. Open the **Network** > **Devices** tab.
2. Hover your mouse over the first column and click on the DeviceView icon ▼.
3. The DeviceView opens as a separate tab.

NOTE: You can also launch a DeviceView from any Device Details menu throughout Extreme Management Center.

Control Tab

Use the following steps to launch DeviceView from the **Control** tab.

1. Open the **Control** > Dashboard tab.
2. Click on the System view.
3. In the Engine Information report, click on an engine IP address to open a DeviceView for the engine.

Extreme Management Center Maps

Use the following steps to launch DeviceView from a map.

1. Open Extreme Management Center Maps and click on a map.
2. In the map, right-click on a device icon and select DeviceView.

Search

Use the following steps to launch DeviceView from the **Search** tab.

1. Open Search and search for a device.
2. In the Overview, right-click on the device icon and select DeviceView.

Related Information

For information on related topics:

- Network Tab

How to Check for Extreme Management Center Updates

Extreme Management Center provides an easy way to access the Extreme Networks website to obtain information about the latest Extreme Networks firmware releases available for download.

Before using the Check for Updates feature, it is important to configure your Update Credentials in the ExtremeNetworks.com Updates options (**Administration** > **Options** > **ExtremeNetworks.com Updates**). These credentials are used to access the website to obtain the update information. First, create an account at ExtremeNetworks.com and define a user name and password for the account credentials. Then you can configure those credentials in the options.

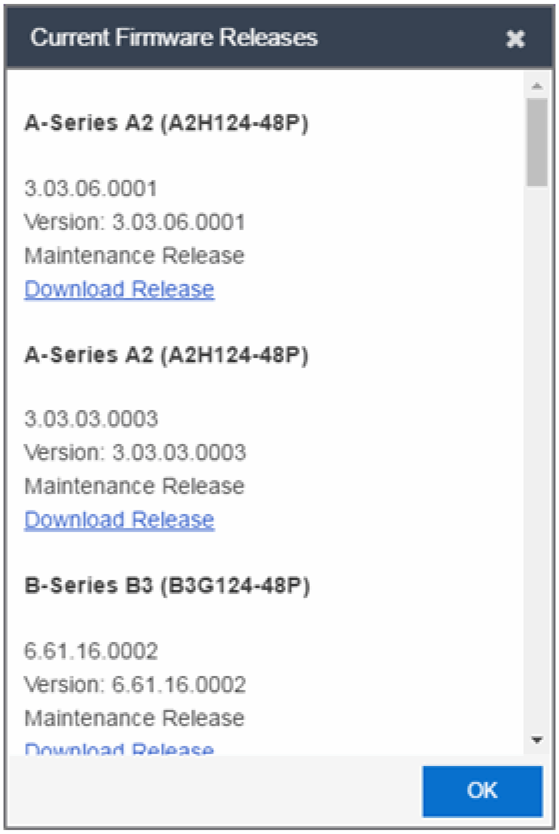
In addition, if your network is behind a firewall, you must also specify in the options the HTTP Proxy server being used, prior to performing an update. Check with your network administrator for the proxy server information.

After you have configured the options, use the following steps to check for firmware updates:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down menu to select **All Devices**, **Maps**, or **Sites**, depending on the devices for which you are updating the firmware. You can also use the drop-down menu to select how the devices are organized (e.g. by IP address, by Device Type).
3. Select the **Devices** tab in the right-panel.
4. Click the **Menu** icon (≡) or right-click in the Devices list.
5. Select **Configuration/Firmware** > **Check For Updates**.

NOTE: You can also right-click a device in the left-panel and select **Configuration/Firmware** > **Check For Updates**.

Extreme Management Center checks ExtremeNetworks.com for the latest firmware versions available for Extreme Networks devices and displays the information in the **Current Firmware Releases** window.



Current Firmware Releases

A-Series A2 (A2H124-48P)

3.03.06.0001
Version: 3.03.06.0001
Maintenance Release
Download Release

A-Series A2 (A2H124-48P)

3.03.03.0003
Version: 3.03.03.0003
Maintenance Release
Download Release

B-Series B3 (B3G124-48P)

6.61.16.0002
Version: 6.61.16.0002
Maintenance Release
Download Release

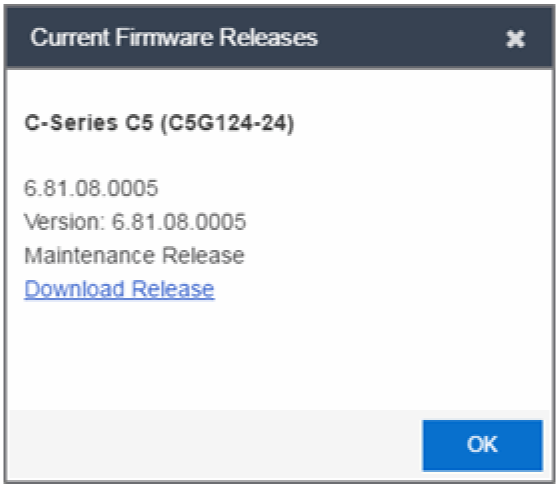
6. Click OK.

   The Firmware icon (▣) in the Updates column of the Devices tab indicates a firmware update is available for the device.

7. Select a device on which you want to update the firmware and click the Menu icon (≡) or right-click the device in the Devices list.

8. Select Configuration/Firmware > View Available Releases.

9. The Current Firmware Releases window displays, which allows you to see the firmware available for that device and download the firmware.



Current Firmware Releases

C-Series C5 (C5G124-24)

6.81.08.0005
Version: 6.81.08.0005
Maintenance Release
Download Release

10. Click on the **Download Release** link to access the website and navigate to the product Firmware download page.
11. Enter your credentials to access the website (use the same credentials configured in the ExtremeNetworks.com Updates options (**Administration** > **Options** > **ExtremeNetworks.com Updates**).

Once you download a firmware version, you can upgrade the firmware on the device.

Related Information

For information on related topics:

- How to Upgrade Firmware
- ExtremeNetworks.com Updates Options

How to Upgrade Firmware in Extreme Management Center

Extreme Management Center allows you to upgrade device firmware for your Extreme Networks devices.

NOTE: Prior to upgrading firmware, you must access the Extreme Networks website to obtain information about the latest Extreme Networks firmware releases available for download.

You can upgrade firmware in one of two ways:

- For a particular device on your network
- For all devices of a device type

You must be a member of an authorization group that includes Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard capability to see this menu option.

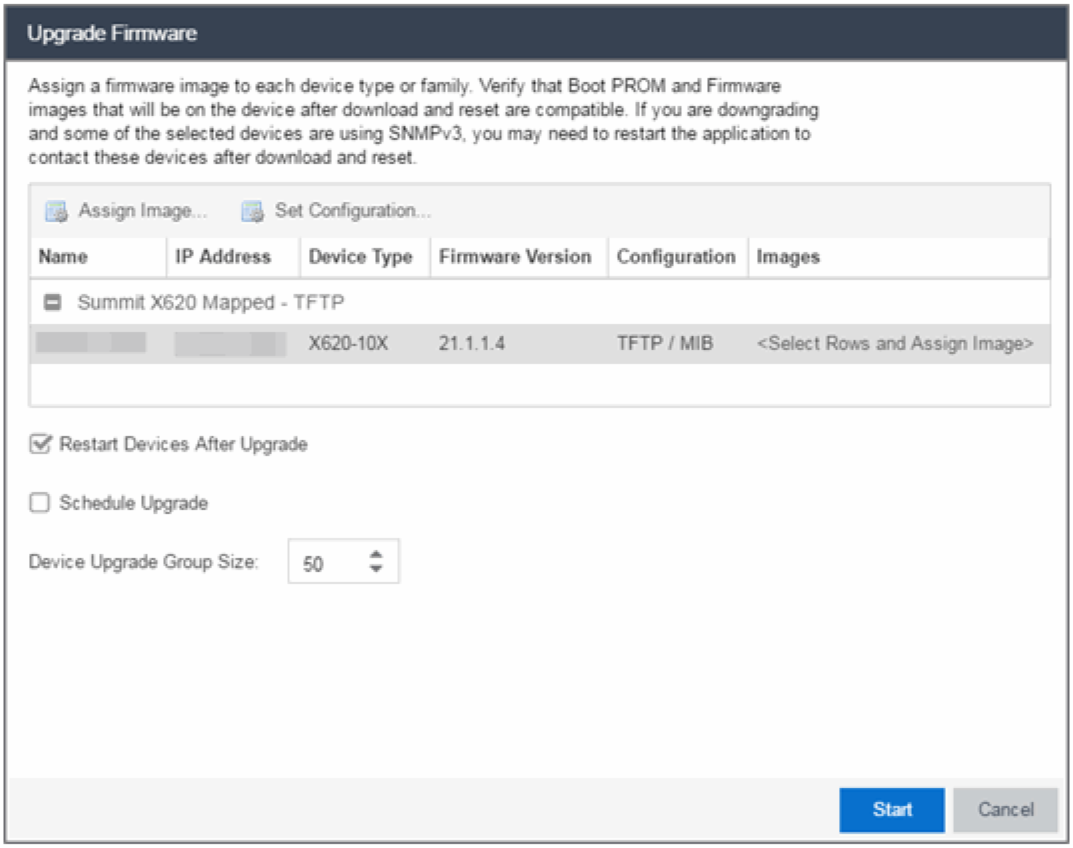
Upgrading for a Device

To upgrade firmware for a particular device:

1. Open the **Network** tab.
2. Select the Devices tab.
3. Select **All Devices** from the left-panel drop-down menu, or select a **Maps** or **Sites**, depending on the location of the device you are upgrading.
4. Select the **Devices** tab in the right-panel.
5. Select the devices for which you are upgrading firmware in the Devices table in the right-hand panel.
6. Click the **Menu** icon (≡) or right-click in the Devices list.
7. Select **Configuration/Firmware** > **Upgrade Firmware**.

NOTE: You can also right-click a single device in the left-panel and select **Configuration/Firmware** > **Upgrade Firmware**.

The Upgrade Firmware window opens, displaying the devices you selected grouped by device family.



Upgrade Firmware

Assign a firmware image to each device type or family. Verify that Boot PROM and Firmware images that will be on the device after download and reset are compatible. If you are downgrading and some of the selected devices are using SNMPv3, you may need to restart the application to contact these devices after download and reset.

Name	IP Address	Device Type	Firmware Version	Configuration	Images
⊟ Summit X620 Mapped - TFTP					
[redacted]	[redacted]	X620-10X	21.1.1.4	TFTP / MIB	<Select Rows and Assign Image>

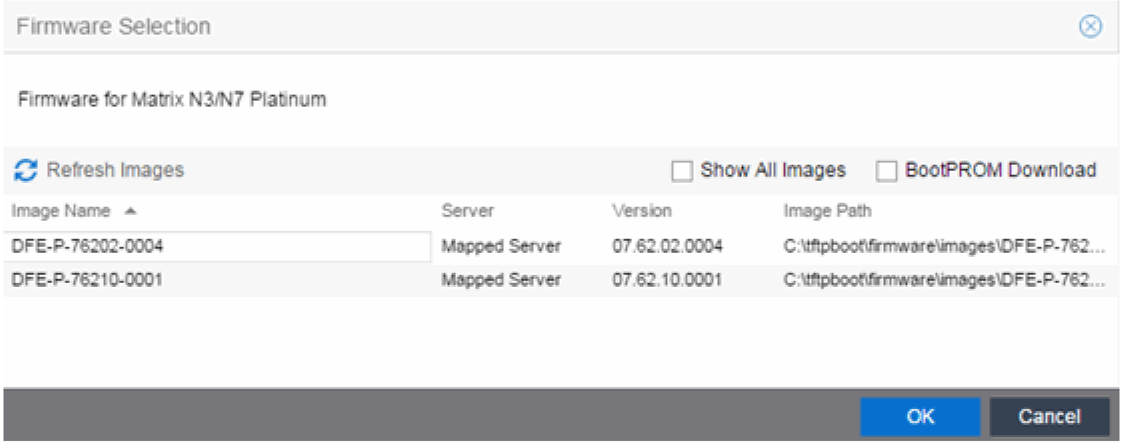
☑ Restart Devices After Upgrade

☐ Schedule Upgrade

Device Upgrade Group Size: 50

8. Select one or more devices and click **Assign Image**.

   The Firmware Selection window opens, displaying the firmware versions compatible with the device type.



Firmware for Matrix N3/N7 Platinum

□ Show All Images □ BootPROM Download

Image Name	Server	Version	Image Path
DFE-P-76202-0004	Mapped Server	07.62.02.0004	C:\tftpboot\firmware\images\DFE-P-762...
DFE-P-76210-0001	Mapped Server	07.62.10.0001	C:\tftpboot\firmware\images\DFE-P-762...

9. Click the **Show All Images** checkbox to show all available firmware images.
10. Select the firmware image to download to the device.
11. After the upgrade operation completes, verify the boot PROM and firmware images on the device are compatible. Refer to the boot PROM and firmware release notes for more information. To upgrade the boot PROM, select the **BootPROM Download** check box in the Firmware Selection window. This clears any images already assigned and only displays boot PROM images for selection.
12. Click **OK**.
13. Repeat the process for all of the devices in the Upgrade Firmware window.

NOTE: Right-click the device in the Upgrade Firmware window to configure how the firmware is downloaded and installed on the device (e.g. to change the server from which the firmware image is downloaded, the file transfer method, or the MIB or script used to download the firmware image).

14. Click the **Restart devices after upgrade** checkbox to automatically restart devices that support restarting immediately after upgrading the firmware image.

NOTES: Clicking the **Restart devices after upgrade** checkbox displays the Supports Restart column in the Upgrade Firmware window. A check mark indicates devices that support this functionality.

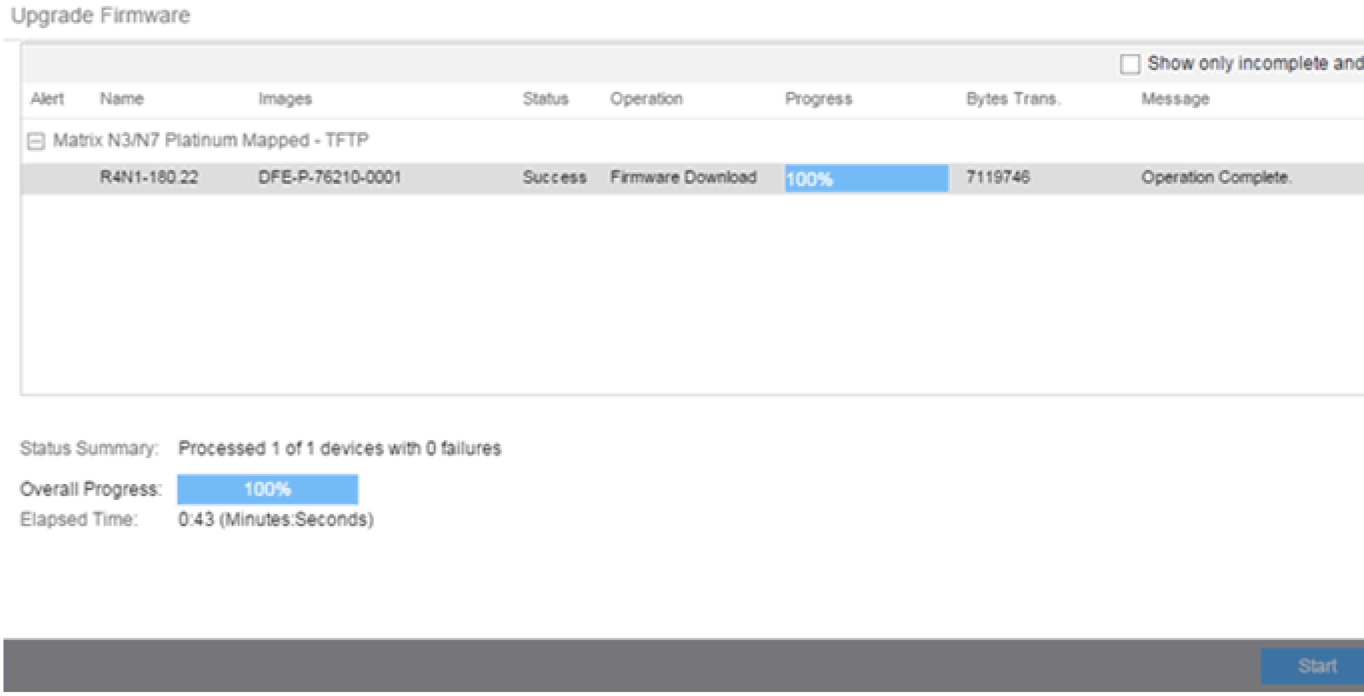
If the **Restart devices after upgrade** checkbox is selected, the **Schedule Upgrade** checkbox is unavailable.

You can also restart a device manually in the Restart Devices window, accessible from the **Network** tab in Extreme Management Center by right-clicking the device and selecting **Configuration/Firmware** > **Restart Device** option.

15. Click the **Schedule Upgrade** checkbox to run the firmware image upgrade at a future date. Clicking this checkbox displays additional fields where you can configure the scheduled upgrade.
    - **Name** — The name for the scheduled upgrade. The default name automatically populates with the creation date and time of the firmware upgrade.
    - **Select Date** — The date and time the upgrade automatically runs. Enter a date in the mm-dd-yyyy format or click the **Calendar** icon 📅 to open a monthly calendar from which you can select the date of the upgrade. Enter the time for the scheduled upgrade or click the drop-down arrow to select the time from a drop-down menu.
    - **Abort on failure** — Clicking this checkbox causes the upgrade to terminate in the event it is not successful.

NOTE: If the **Schedule Upgrade** checkbox is selected, the **Restart devices after upgrade** checkbox is unavailable.

16. Enter the number of downloads upgraded simultaneously in the **Device upgrade group size** field. Enter a value of **1** to have the downloads performed serially (one device at a time).
17. Click **Start** if you are upgrading the firmware immediately or **Schedule** if the upgrade is scheduled for a future date.
18. If upgrading the firmware image immediately, a progress column appears on the Upgrade Firmware window. Once the upgrade is complete, a Status section appears, displaying whether the upgrade occurred successfully.



Upgrade Firmware

☐ Show only incomplete and

Alert	Name	Images	Status	Operation	Progress	Bytes Trans.	Message
⊟ Matrix N3/N7 Platinum Mapped - TFTP							
	R4N1-180.22	DFE-P-76210-0001	Success	Firmware Download	100%	7119746	Operation Complete.

Status Summary: Processed 1 of 1 devices with 0 failures

Overall Progress: 100%

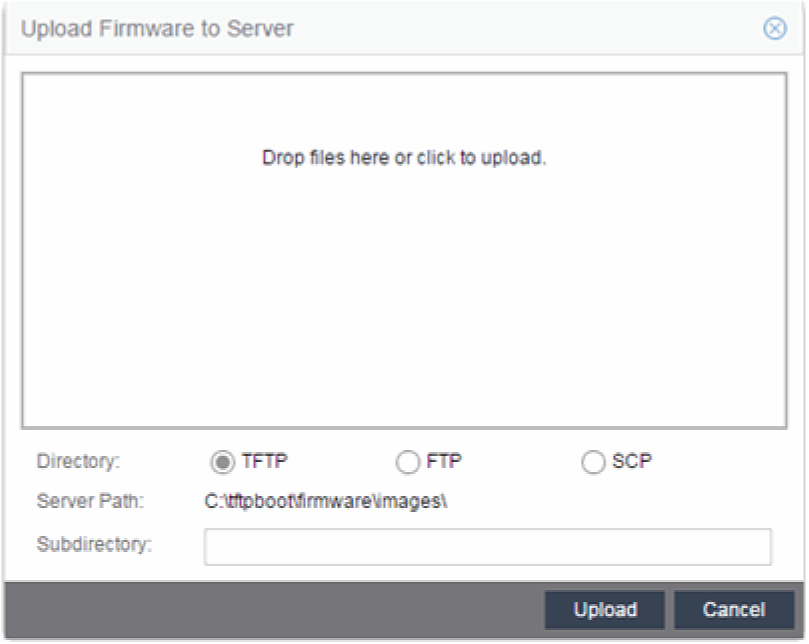
Elapsed Time: 0:43 (Minutes:Seconds)

19. Click **Close**.

Upgrading for a Device Type

To upgrade the firmware for all devices of a particular device type:

1. Open the **Network** tab.
2. Select the Firmware tab.
3. Select the device type from the Firmware tree in the left panel.
4. Upload the firmware or boot PROM image, if necessary.
    a. Click the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the Extreme Management Center server.


Upload Firmware to Server
Drop files here or click to upload.
Upload
Cancel

Directory: ● TFTP ○ FTP ○ SCP

Server Path: C:\tftpboot\firmware\images\

Subdirectory:

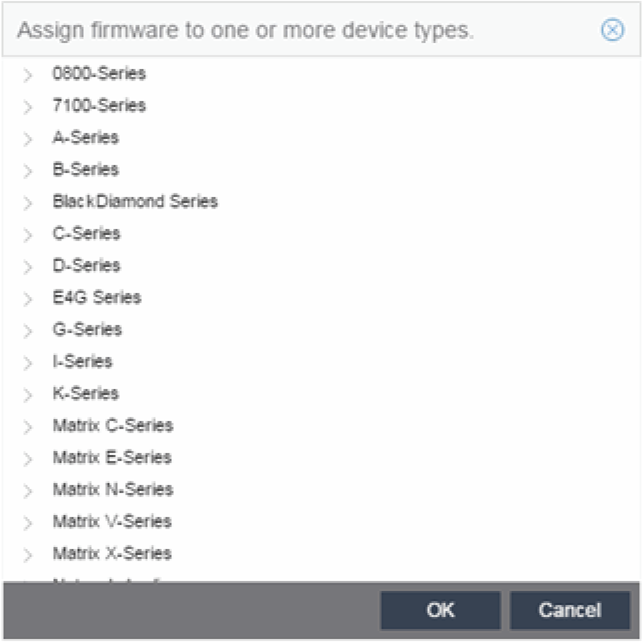
b. Drag the file or files into the box in the main part of the window or click the box to open a window from which you can navigate to the appropriate directory.

c. Select **TFTP**, **FTP**, or **SCP** to indicate whether you are upgrading the firmware or boot PROM image using a TFTP, FTP, or SCP server, respectively.

d. Type the Subdirectory within the Server Path where the firmware or boot PROM images are uploaded.

e. Click the **Upload** button.
A status bar displays over the file icon and a checkmark indicates when the upload is complete. Anyone with access to Extreme Management Center is now able to download the image file to a device.

5. Right-click the firmware or boot PROM image from the Device Type Images section of the window and select **Assign Firmware** from the menu.
The Assign Firmware to One or More Device Types window appears.



Assign firmware to one or more device types.

- 0800-Series
- 7100-Series
- A-Series
- B-Series
- BlackDiamond Series
- C-Series
- D-Series
- E4G Series
- G-Series
- I-Series
- K-Series
- Matrix C-Series
- Matrix E-Series
- Matrix N-Series
- Matrix V-Series
- Matrix X-Series

6. Select the device type to which to assign the firmware or boot PROM image.
7. Click **OK**.

If you did not select **Restart devices after upgrade**, restart your devices.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware Tab

How to Restart a Device

Use the **Devices** tab to restart a single device or multiple devices. The tab lets you restart devices that support Timed Restart as well as those devices that do not. Timed Restart lets you configure your restart operation with a time delay, so that the actual device restarts take place at a later time.

To restart a device:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down menu to select **All Devices**, **Maps**, or **Sites**, depending on the devices you are restarting. You can also use the drop-down menu to select how the devices are organized (e.g. by IP address, by Device Type).
3. Select the **Devices** tab in the right-panel.
4. Select the device or devices you want to restart (using the **Ctrl** or **Shift** keys).
5. Click the **Menu** icon (≡) or right-click in the Devices list.
6. Select **Configuration/Firmware** > **Restart Device**.

   NOTE: You can also right-click a single device in the left-panel and select **Configuration/Firmware** > **Restart Device**.

   The **Restart Devices** window displays.
7. Select the devices you want to restart by clicking the checkbox in the **Selected** column.

   NOTE: The **Restart Devices** window contains additional fields for devices that support timed restart.
8. Select the date and time you want to restart the device for devices that support timed restart using the **Restart Time** fields. This field defaults to the current date and time, so to restart the devices now, do not change this field.
9. Click **Start** to initiate the device restarts or to schedule a future device restart. **Elapsed Time** displays the elapsed time since beginning the restart process.
10. Click **Finish** to close the window.

Related Information

For information on related topics:

- How to Upgrade Firmware
- Restart Device Window

▲

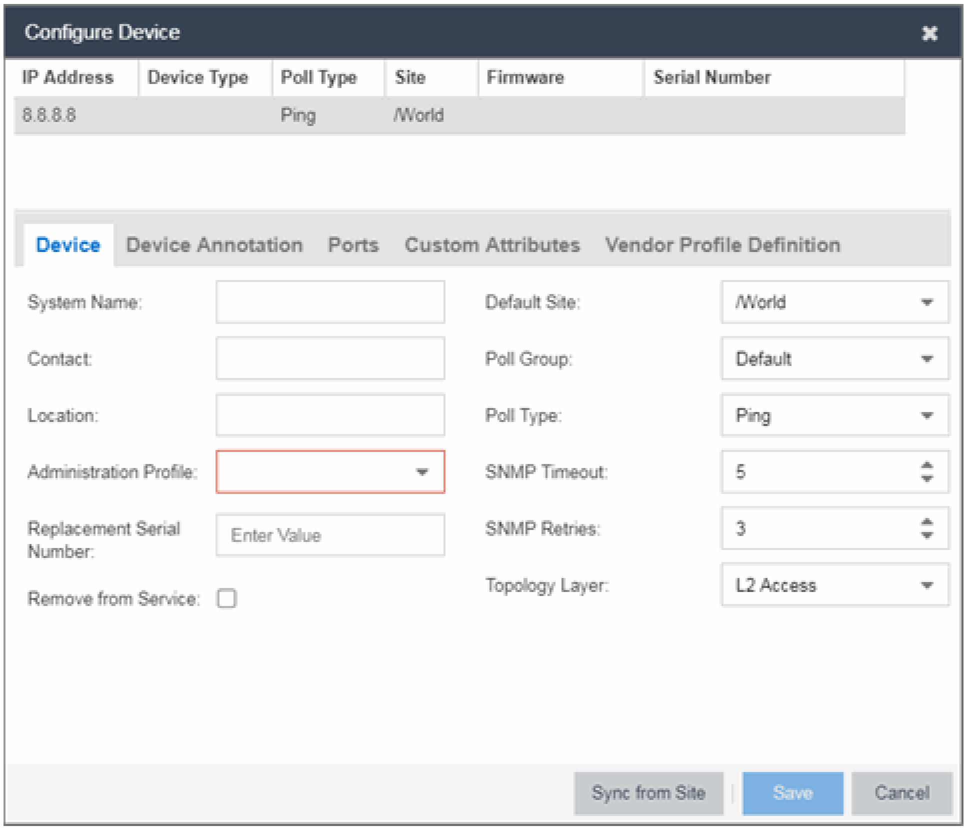
How to Create and Edit a VLAN in Extreme Management Center

This section outlines how to create and edit a VLAN. From the **Network** tab, you can:

- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

1. Launch Extreme Management Center.
2. Open the **Network** > **Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device** > **Configure Device**.
   The **Configure Device** window opens.



IP Address	Device Type	Poll Type	Site	Firmware	Serial Number
8.8.8.8		Ping	/World		

System Name:

Contact:

Location:

Administration Profile:

Replacement Serial Number: Enter Value

Remove from Service: □

Default Site: /World

Poll Group: Default

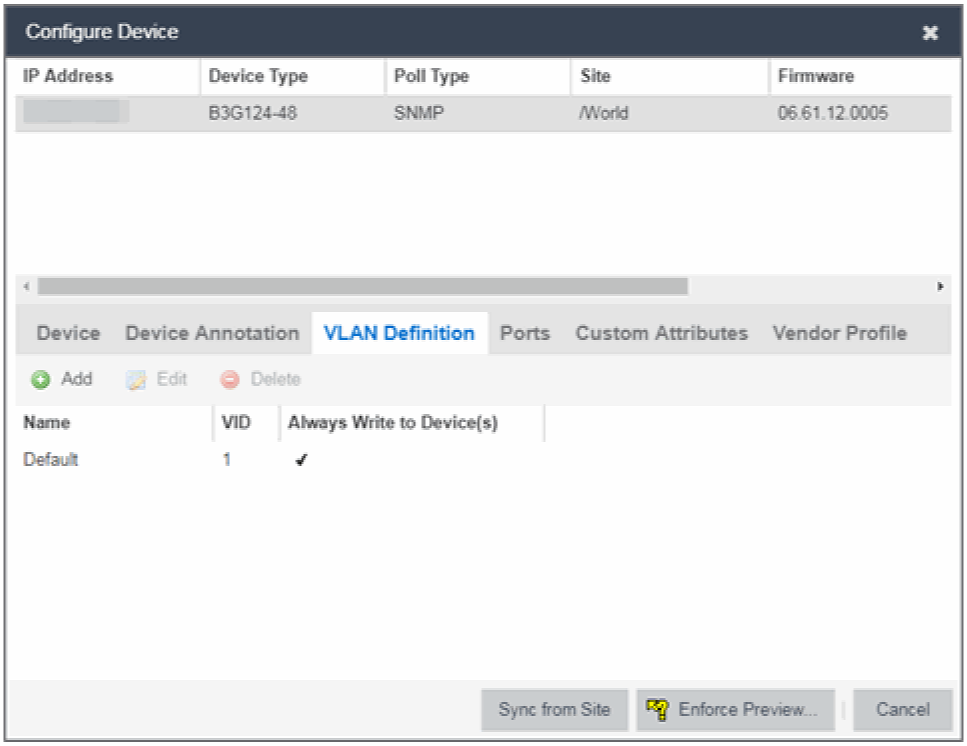
Poll Type: Ping

SNMP Timeout: 5

SNMP Retries: 3

Topology Layer: L2 Access

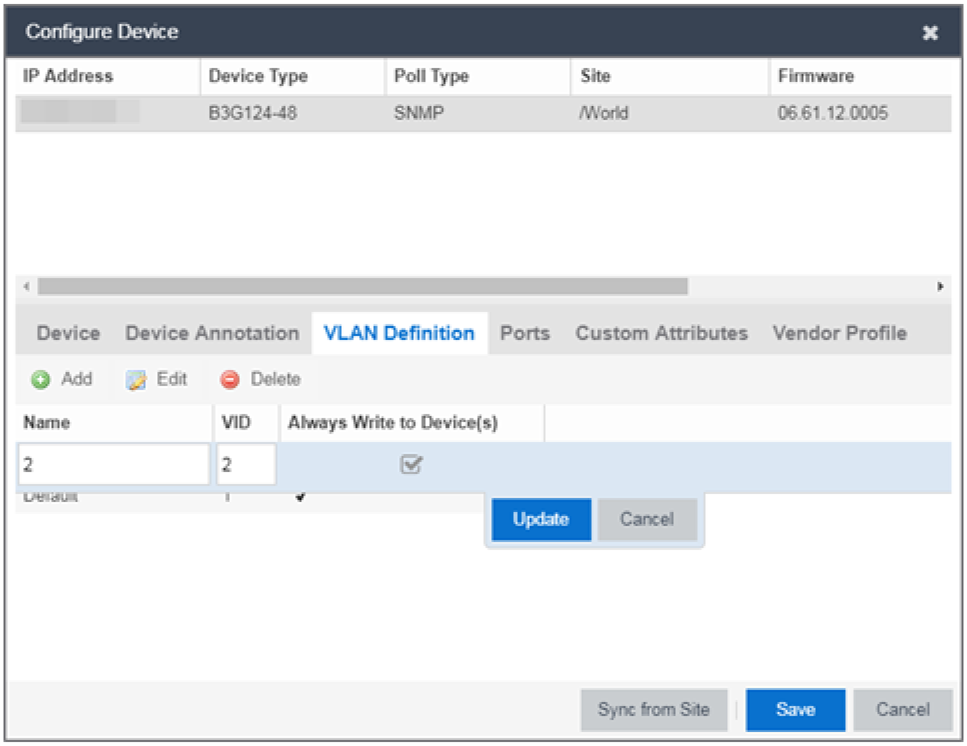
4. Select the **VLAN Definition** tab.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

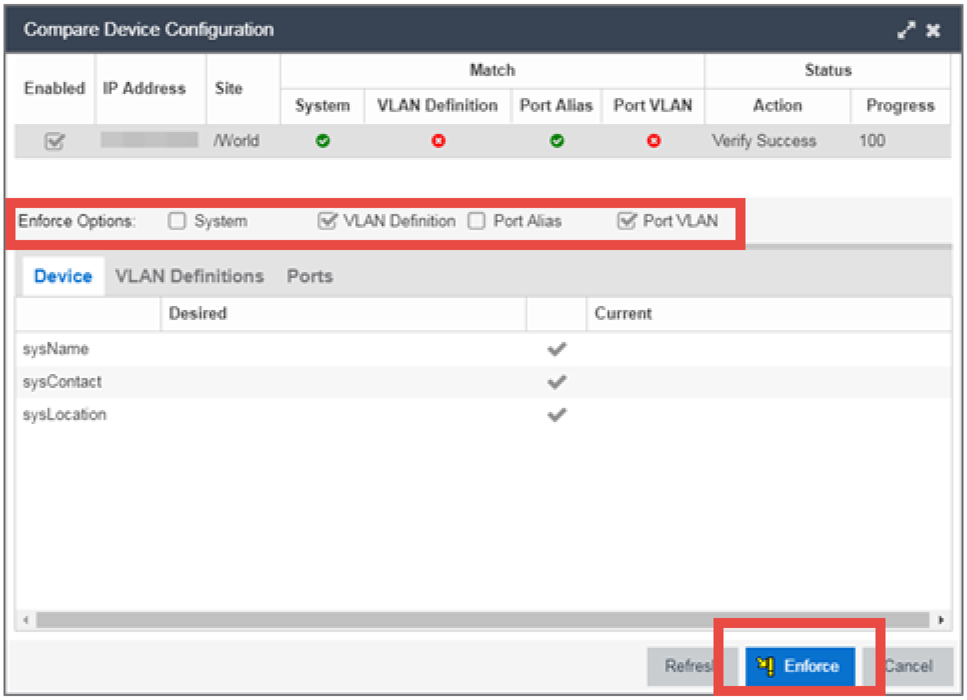
5. Click the **Add** button.
6. Enter the **Name** and the VID for the new VLAN.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
2	2	☑
Default	1	✓

7. Select **Update**.
   The new VLAN is added to the list.
8. Select **Enforce Preview**.
9. Under the Enforce Options, select the **VLAN Definition** checkbox and select **Enforce**.



Enabled	IP Address	Site	Match				Status	
			System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
☑	[redacted]	/World	🟢	🔴	🟢	🔴	Verify Success	100

Enforce Options: □ System ☑ VLAN Definition □ Port Alias ☑ Port VLAN

	Desired		Current
sysName		✓	
sysContact		✓	
sysLocation		✓	

NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

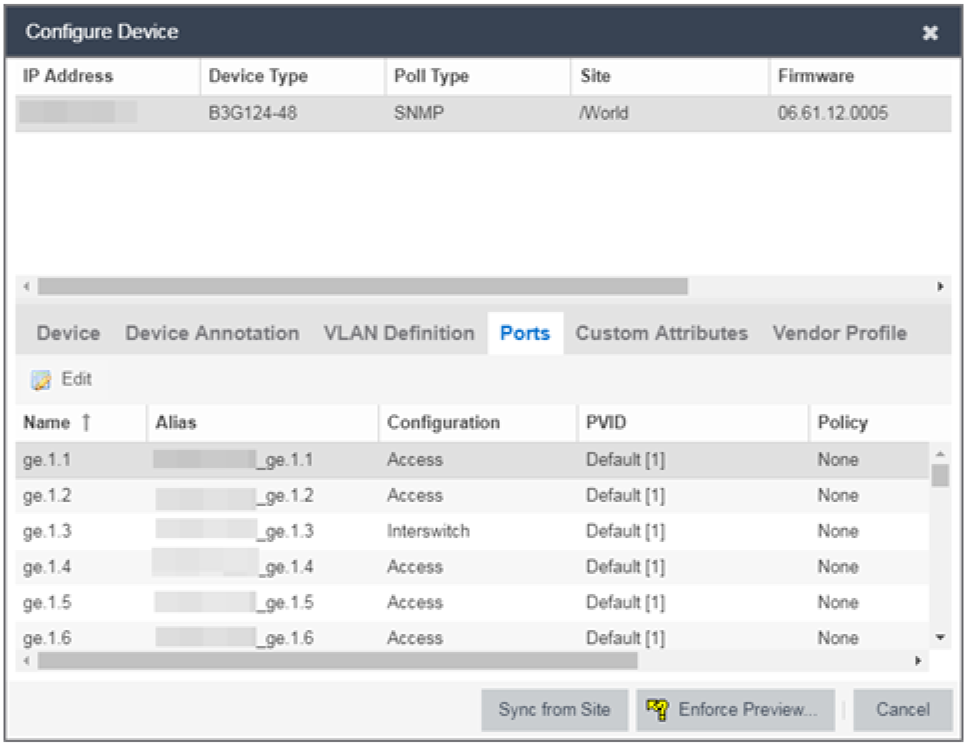
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.

3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.
5. Select the **Ports** tab.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name ↑	Alias	Configuration	PVID	Policy
ge.1.1	[redacted]_ge.1.1	Access	Default [1]	None
ge.1.2	[redacted]_ge.1.2	Access	Default [1]	None
ge.1.3	[redacted]_ge.1.3	Interswitch	Default [1]	None
ge.1.4	[redacted]_ge.1.4	Access	Default [1]	None
ge.1.5	[redacted]_ge.1.5	Access	Default [1]	None
ge.1.6	[redacted]_ge.1.6	Access	Default [1]	None

6. Select the Port on which you are configuring the VLAN.
7. Select **Edit**.
   The Port is now configurable.
8. Change the **PVID**, **Tagged**, and **Untagged** options to configure the VLAN onto the port.
9. Click **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

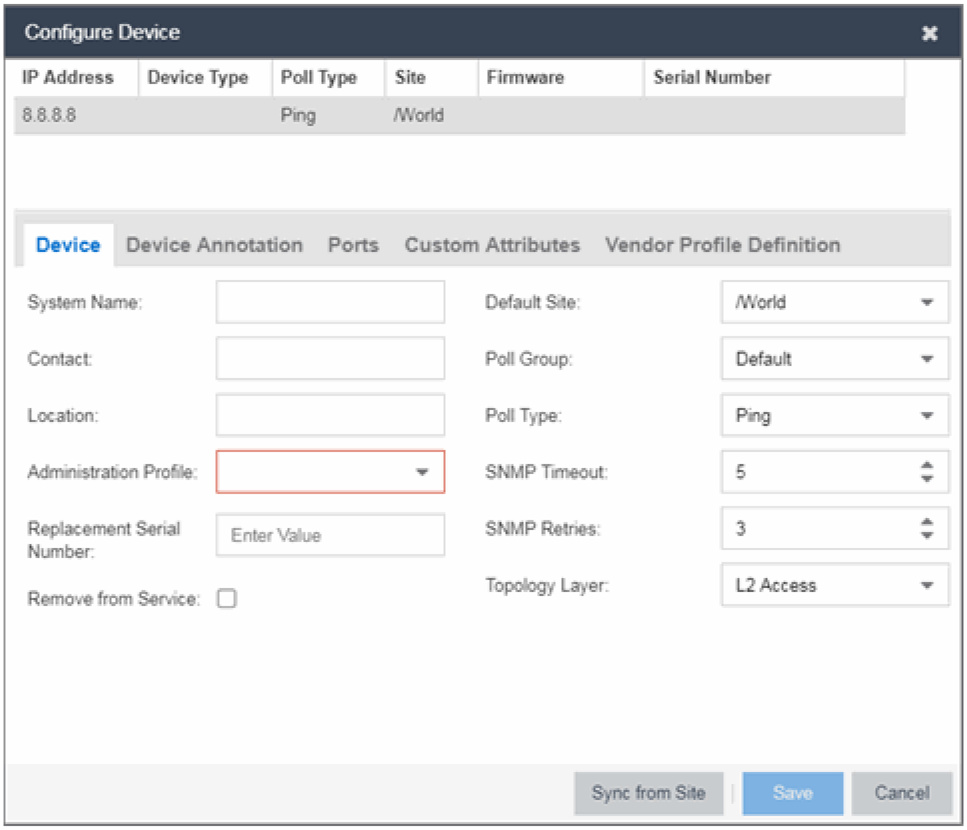
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now configured to the Ports.

To edit the name of a VLAN:

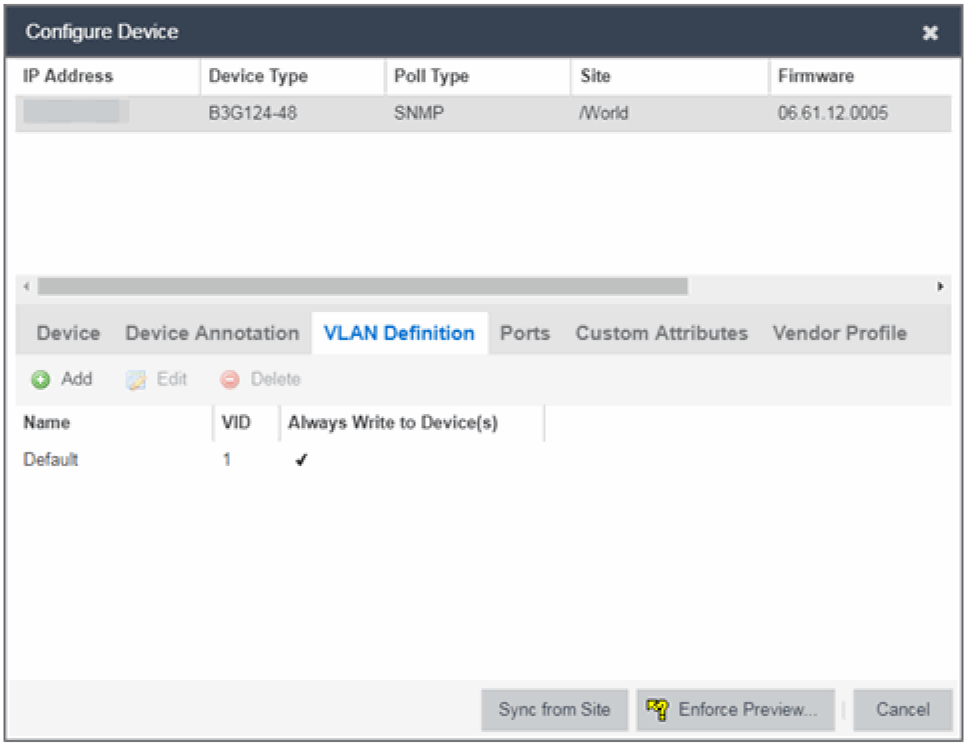
1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.



IP Address	Device Type	Poll Type	Site	Firmware	Serial Number
8.8.8.8		Ping	/World		

System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service: ☐		Topology Layer:	L2 Access

5. Click the **VLAN Definition** tab.



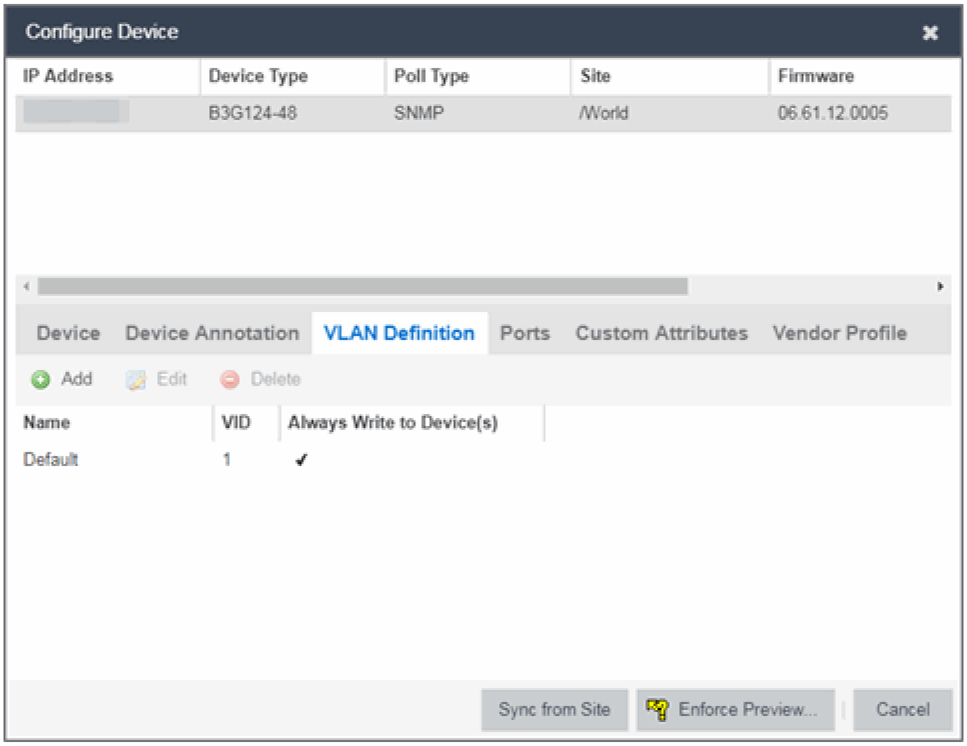
IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Click **Update**.
   The Edit pane closes.
9. Click **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.
4. Click the **VLAN Definition** tab.
   The VLAN Definition pane opens.



IP Address	Device Type	Poll Type	Site	Firmware
[redacted]	B3G124-48	SNMP	/World	06.61.12.0005

Name	VID	Always Write to Device(s)
Default	1	✓

5. Select the VLAN and click **Delete**.

Related Information

For information on related topics:

- Maps
- Devices tab

How to Add a New Regime in Extreme Management Center

The Governance tab provides you with regimes that include predefined audit tests. You can also create your own regimes, composed of audit tests you can copy from existing regimes, or configure yourself.

To create a new regime:

1. Open the **Governance** > Audit Tests tab.
2. Click the **Menu** icon (☰) and select **Add** > **Regime**.

   The Create Regime window displays.
3. Enter a **Regime Name**, describing the overarching standard or regulation against which you are testing compliance.
4. Enter a **Description** for the regime, if necessary.
5. Select **Test Wireless Events** to include wireless events in the governance audit.

   > **NOTE:** Because of the number of wireless events potentially stored by Extreme Management Center, wireless events are not included in a governance audit the first time it is run. Once the governance audit is run the first time, older wireless events are moved, so older events are not included in the results.
6. Click **Save**.
7. Copy existing audit tests to the new regime, if necessary.
   a. Right-click the audit test in left-panel and selecting **Copy Audit Test**.

      The **Copy Audit Test** window displays.

   b. Enter a new name for the audit test, if necessary.

   c. Select the new regime in the **Regime** drop-down menu.

   d. Select the device type to which the audit test applies in the **Device Type** drop-down menu.

   e. Click **Copy**.
8. Create your own audit tests.
   a. Click the **Menu** icon (☰) and select **Add** > **Audit Test**.

   b. Complete the fields in the Audit Test Editor tab to test for a device configuration.

   c. Complete the fields in the Dependent Tests tab, if necessary.

   d. Click **Save**.

Your custom regime is now available on the Governance tab.

Related Information

For information on related tabs:

- Governance Overview
- Diagnostics

How to Obtain and Apply a Governance License in Extreme Management Center

To use the Governance tab in Extreme Management Center, an additional license is required.

To obtain and apply the license in Extreme Management Center:

1. Contact your sales representative to purchase an IGE (Information Governance Engine) license.

   An email voucher is generated and sent to you with instructions.
2. Create an Extreme Networks Support Portal account, if necessary.
   a. Open a browser and go to https://secure.extremenetworks.com/.
   b. Enter your information and click **Create An Account**.

      An email is sent to you with instructions to activate your account.
   c. Click the link in your email.

      The Portal - Account Activation web page displays.
   d. Enter your **Email Address** and the **Activation Code** included in your activation email, if they do not automatically populate.
   e. Click **Activate**.
3. Access the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding.
4. Enter your **Email** and **Password** and click **Log In**.

5. Click **Generate License**.

   The Generate License window displays.
6. Enter your **Voucher ID** from the email voucher sent to you and click **Next**.
7. Select the **Terms and Conditions** checkbox and click **Submit**.

   A window displays with your software license key.
8. Copy the license key from the window.
9. Open Extreme Management Center.
10. Access the **Administration** > **Diagnostics** tab.
11. Select **Server** > **Server Licenses** in the left-panel.

    The **Server Licenses** panel displays.
12. Click **Add**.

    The **Add License** window displays.
13. Paste the license key you copied in Step 9 and click **OK**.
14. Restart Extreme Management Center.
15. The **Governance** tab is now available in the menu, allowing you to use governance audit functionality.

Related Information

For information on related tabs:

- Governance Overview
- Diagnostics

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new devices to your network and configure them in Extreme Management Center.

Typically, when adding a new device to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Reference Firmware Image Location
- Download XMODs
- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center to automatically update your device's firmware and application versions. When upgrading the firmware image on your device, access the appropriate firmware image for your version from ExtremeNetworks.com and save it on your server to a directory you configure in Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

For the device to recognize a new version is available, the firmware image must be downloaded from ExtremeNetworks.com to your server and saved in a directory you configure in Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **Options** tab.
2. Select **Inventory Manager** in the left panel.
3. Enter the **Firmware Directory Path** in either the FTP Server Properties, SCP Server Properties, or TFTP Properties section of the right panel, depending on the file transfer settings used.
4. Download the latest firmware image for your device from ExtremeNetworks.com and save it in the specified directory.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center server to the device.

1. Access the **Network** > **Firmware** tab.
2. Expand the **Device Type** navigation tree in the left-panel for the device family you are configuring and select the folder for the type of device.
3. Right-click the firmware file you downloaded (specified in the section above) and select **Set as Reference Image**.

   NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality as well as provide bug fixes for existing features. Like firmware image upgrades, they are posted by Extreme Networks on github and ExtremeNetworks.com. Save XMODs in the directory you specify in the **Firmware Directory Path** field. Do not set an XMOD as the reference image.

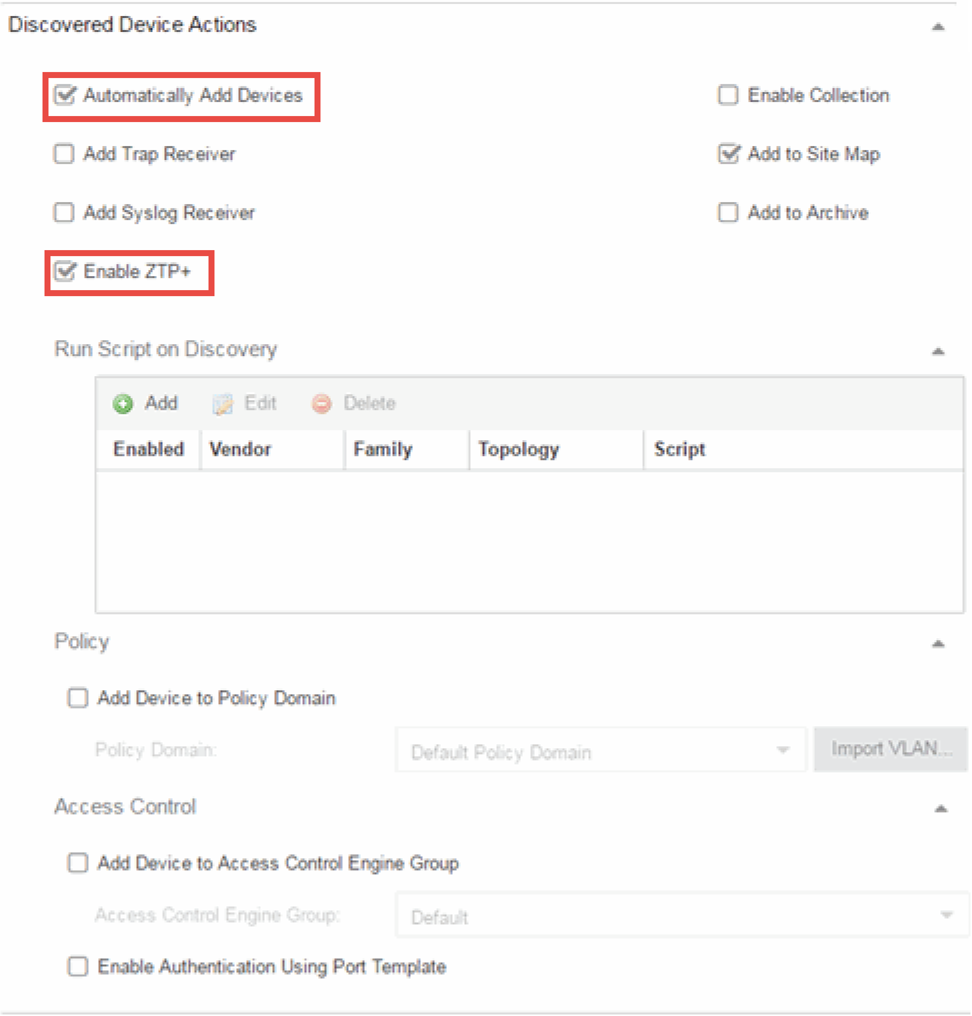
IMPORTANT: ExtremeXOS devices on which version 21.1.1.4 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
2. Expand the World Site navigation tree and select the map in the left panel into which you are adding the devices.
3. Select the **Site** tab in the right panel.
4. Select the **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



Discovered Device Actions

☑ Automatically Add Devices

☐ Enable Collection

☐ Add Trap Receiver

☑ Add to Site Map

☐ Add Syslog Receiver

☐ Add to Archive

☑ Enable ZTP+

Run Script on Discovery

Enabled	Vendor	Family	Topology	Script

Policy

☐ Add Device to Policy Domain

Policy Domain: Default Policy Domain

Access Control

☐ Add Device to Access Control Engine Group

Access Control Engine Group: Default

☐ Enable Authentication Using Port Template

5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

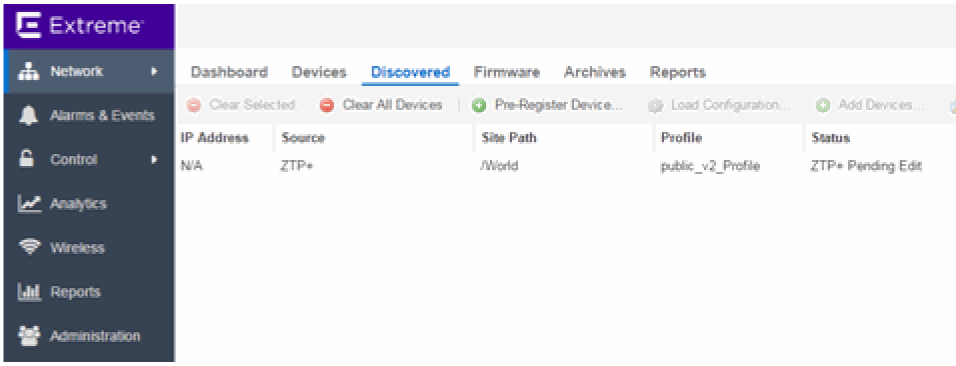
Adding the Device to the Extreme Management Center Database

Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the Firmware tab and set as Reference images, they are automatically installed.
2. Open the **Network** > Discovered tab in Extreme Management Center.

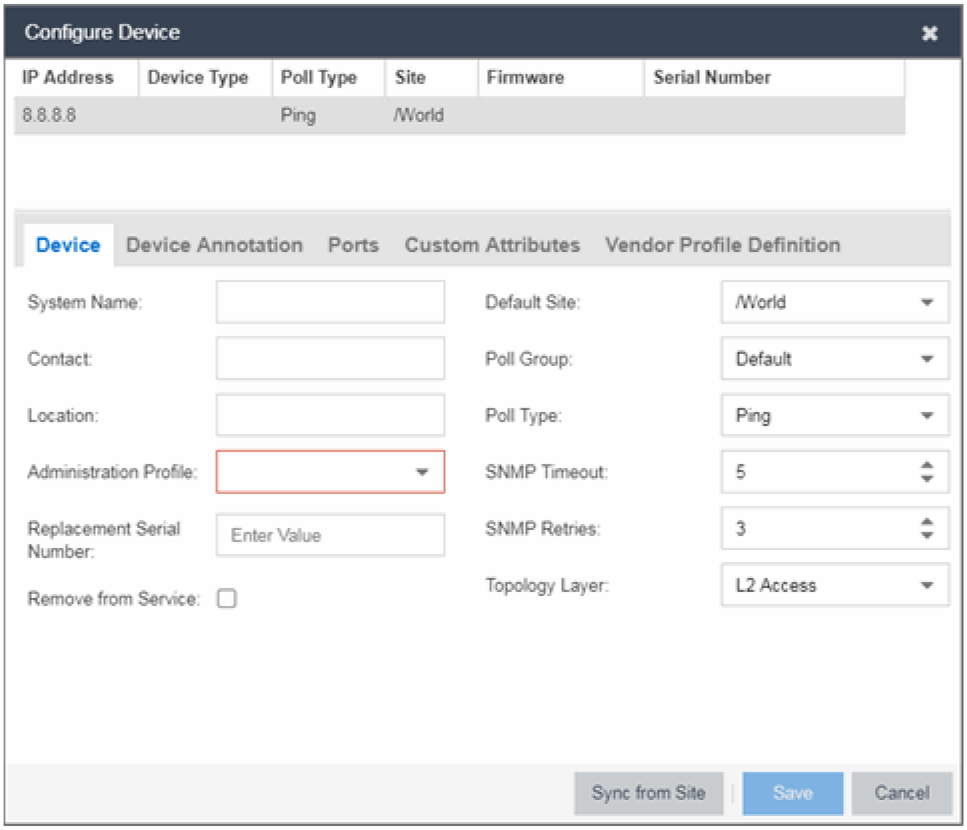
   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



IP Address	Source	Site Path	Profile	Status
N/A	ZTP+	/World	public_v2_Profile	ZTP+ Pending Edit

3. Select the device and click the **Configure Devices** button.

   The **Configure Device** window opens.



IP Address	Device Type	Poll Type	Site	Firmware	Serial Number
8.8.8.8		Ping	/World		

System Name:		Default Site:	/World
Contact:		Poll Group:	Default
Location:		Poll Type:	Ping
Administration Profile:		SNMP Timeout:	5
Replacement Serial Number:	Enter Value	SNMP Retries:	3
Remove from Service:	☐	Topology Layer:	L2 Access

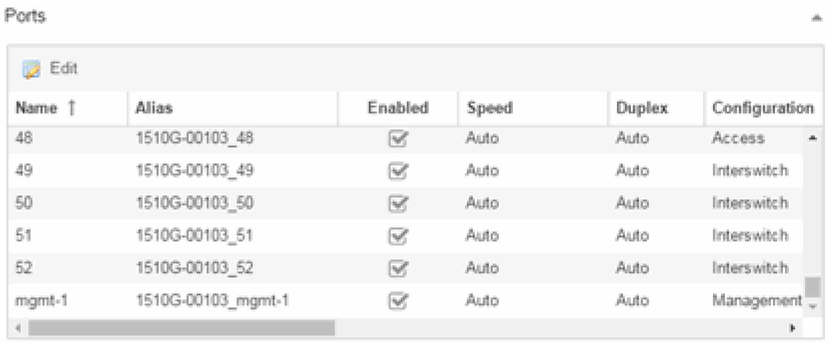
4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.

7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

NOTE: Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.
10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.



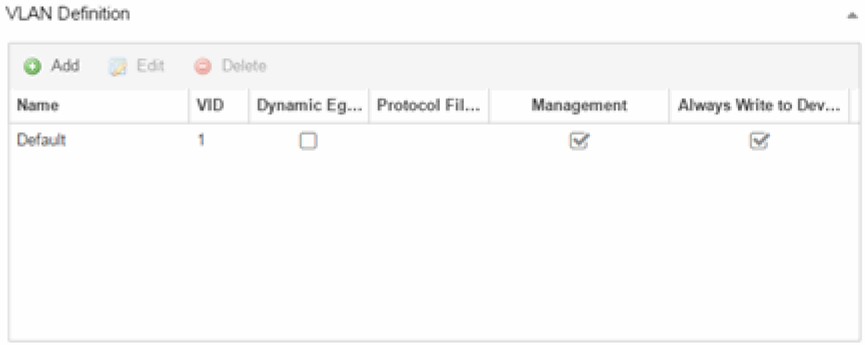
Name ↑	Alias	Enabled	Speed	Duplex	Configuration
48	1510G-00103_48	☑	Auto	Auto	Access
49	1510G-00103_49	☑	Auto	Auto	Interswitch
50	1510G-00103_50	☑	Auto	Auto	Interswitch
51	1510G-00103_51	☑	Auto	Auto	Interswitch
52	1510G-00103_52	☑	Auto	Auto	Interswitch
mgmt-1	1510G-00103_mgmt-1	☑	Auto	Auto	Management

11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking the **Add** and **Delete** buttons, respectively.

    a. Enter the port **Alias**.
    b. Select the port **Configuration**, which is its role or purpose for the device.
        - **Access** — The port provides access to end-systems.
        - **Interswitch** — The port connects the switch to another switch.
        - **Management** — The port is used to manage the network via Extreme Management Center.
    c. Enter a VLAN ID for the port in the **PVID** field.
    d. Configure the port **Speed** and **Duplex**.
12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



Name	VID	Dynamic Eg...	Protocol Fil...	Management	Always Write to Dev...
Default	1	☐		☑	☑

13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

    NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the device remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the device, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center database.

    In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the device resets and allows the process to restart.

The device **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Configure Device
- Devices

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new devices to your network and configure them in Extreme Management Center.

Typically, when adding a new device to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Download XMODs

- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center to automatically update your device's firmware and application versions. When upgrading the firmware image on your device, access the appropriate firmware image for your version from ExtremeNetworks.com and save it on your server to a directory you configure in Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

For the device to recognize a new version is available, the firmware image must be downloaded from ExtremeNetworks.com to your server and saved in a directory you configure in Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **Options** tab.
2. Select **Inventory Manager** in the left panel.
3. Enter the **Firmware Directory Path** in either the FTP Server Properties, SCP Server Properties, or TFTP Properties section of the right panel, depending on the file transfer settings used.
4. Download the latest firmware image for your device from ExtremeNetworks.com and save it in the specified directory.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center server to the device.

1. Access the **Network** > **Firmware** tab.
2. Expand the **Device Type** navigation tree in the left-panel for the device family you are configuring and select the folder for the type of device.
3. Right-click the firmware file you downloaded (specified in the section above) and select **Set as Reference Image**.

NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality as well as provide bug fixes for existing features. Like firmware image upgrades, they are posted by Extreme Networks on github and ExtremeNetworks.com. Save XMODs in the directory you specify in the **Firmware Directory Path** field. Do not set an XMOD as the reference image.

IMPORTANT: ExtremeXOS devices on which version 21.1.1.4 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

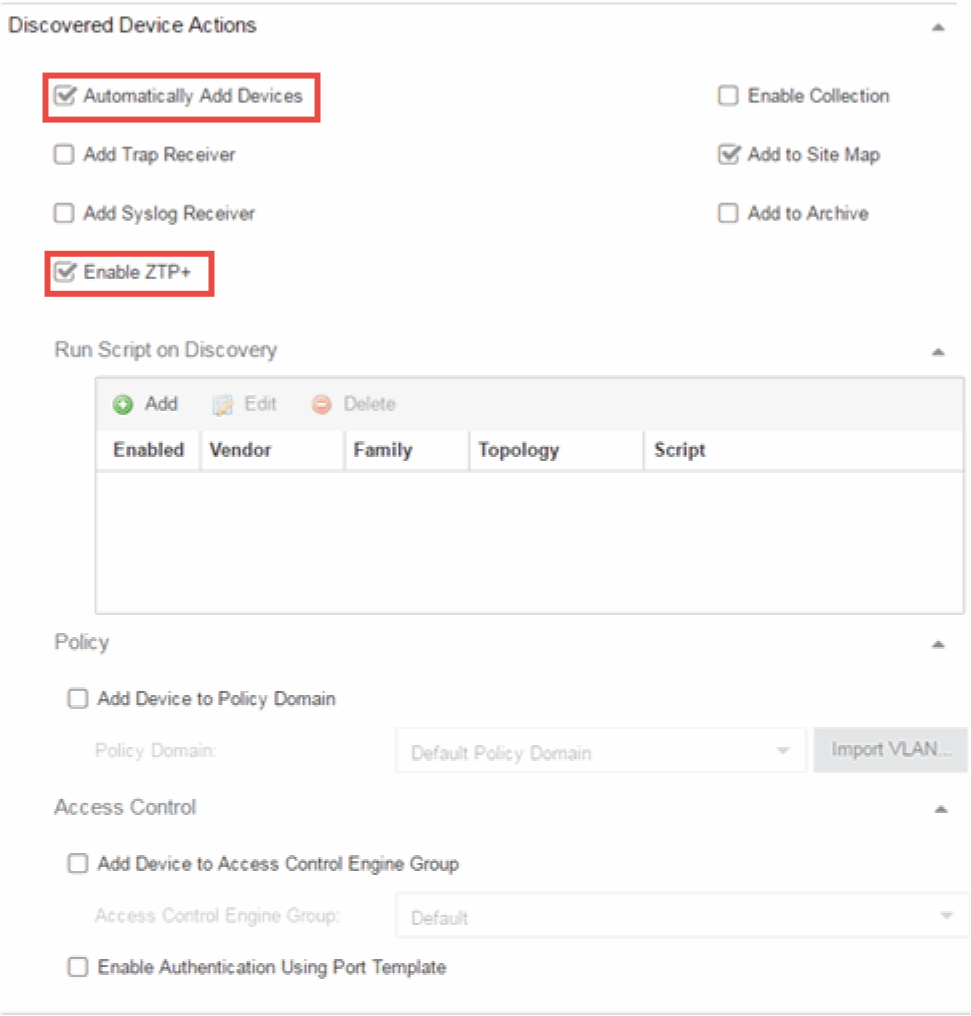
If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
2. Expand the World Site navigation tree and select the map in the left panel into which you are adding the devices.
3. Select the **Site** tab in the right panel.

4. Select the **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



Discovered Device Actions

☑ Automatically Add Devices
☐ Add Trap Receiver
☐ Add Syslog Receiver
☑ Enable ZTP+
☐ Enable Collection
☑ Add to Site Map
☐ Add to Archive

Run Script on Discovery

Enabled	Vendor	Family	Topology	Script

Policy

☐ Add Device to Policy Domain
Policy Domain: Default Policy Domain

Access Control

☐ Add Device to Access Control Engine Group
Access Control Engine Group: Default
☐ Enable Authentication Using Port Template

5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.

8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

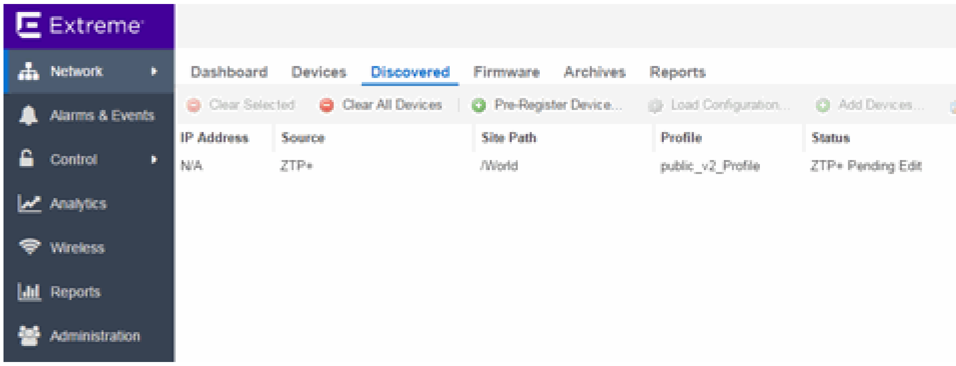
Adding the Device to the Extreme Management Center Database

Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the Firmware tab and set as Reference images, they are automatically installed.
2. Open the **Network** > Discovered tab in Extreme Management Center.

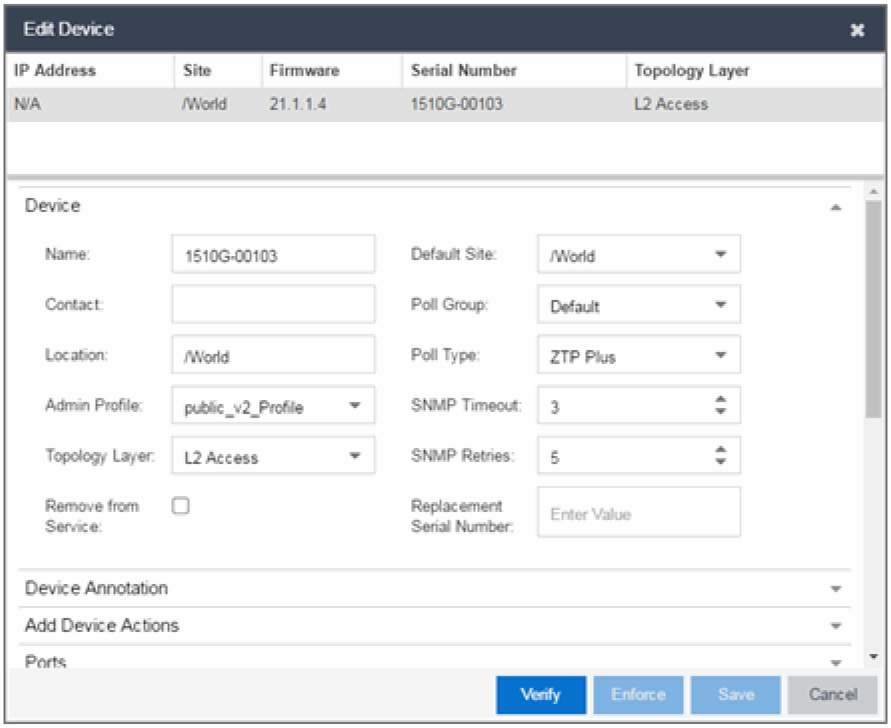
   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



IP Address	Source	Site Path	Profile	Status
N/A	ZTP+	/World	public_v2_Profile	ZTP+ Pending Edit

3. Select the device and click the **Edit Devices** button.

   The **Edit Device** window opens.



IP Address	Site	Firmware	Serial Number	Topology Layer
N/A	/World	21.1.1.4	1510G-00103	L2 Access

Name:	1510G-00103	Default Site:	/World
Contact:		Poll Group:	Default
Location:	/World	Poll Type:	ZTP Plus
Admin Profile:	public_v2_Profile	SNMP Timeout:	3
Topology Layer:	L2 Access	SNMP Retries:	5
Remove from Service:	☐	Replacement Serial Number:	Enter Value

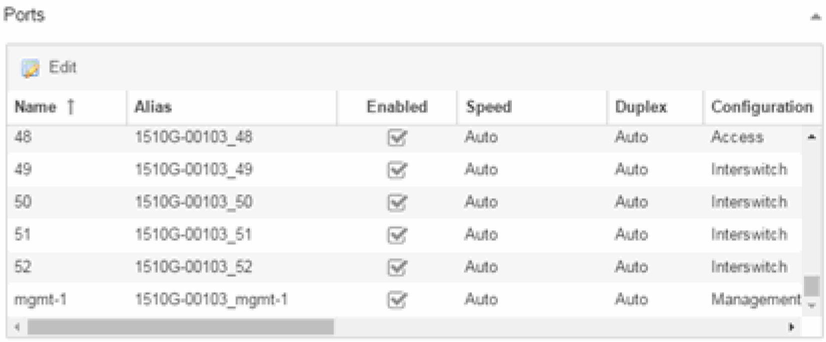
4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.

7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

> **NOTE:** Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.
10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.



Ports

Edit

Name ↑	Alias	Enabled	Speed	Duplex	Configuration
48	1510G-00103_48	☑	Auto	Auto	Access
49	1510G-00103_49	☑	Auto	Auto	Interswitch
50	1510G-00103_50	☑	Auto	Auto	Interswitch
51	1510G-00103_51	☑	Auto	Auto	Interswitch
52	1510G-00103_52	☑	Auto	Auto	Interswitch
mgmt-1	1510G-00103_mgmt-1	☑	Auto	Auto	Management

11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking the **Add** and **Delete** buttons, respectively.

    a. Enter the port **Alias**.

    b. Select the port **Configuration**, which is its role or purpose for the device.

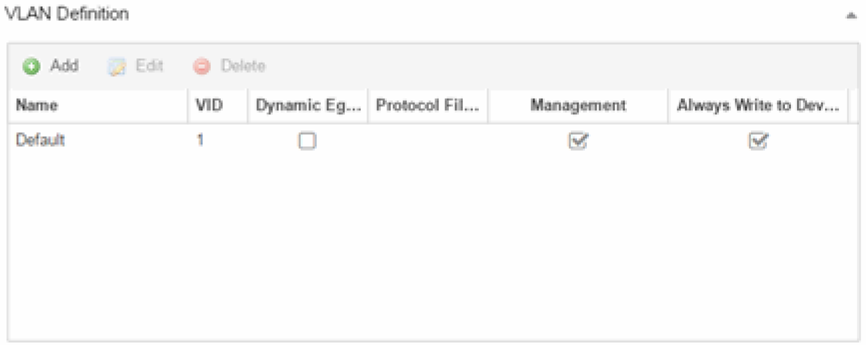
       - **Access** — The port provides access to end-systems.
       - **Interswitch** — The port connects the switch to another switch.
       - **Management** — The port is used to manage the network via Extreme Management Center.

    c. Enter a VLAN ID for the port in the **PVID** field.

    d. Configure the port **Speed** and **Duplex**.

12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



Name	VID	Dynamic Eg...	Protocol Fil...	Management	Always Write to Dev...
Default	1	□		☑	☑

13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the device remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the device, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the device resets and allows the process to restart.

The device **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Edit Device
- Devices

ZTP+ Analytics Engine Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new Application Analytics engines to your network and configure them in Extreme Management Center.

Typically, when adding a new engine to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Download XMODs

- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center to automatically update your device's firmware and application versions. When upgrading the firmware image on your device, access the appropriate firmware image for your version from ExtremeNetworks.com and save it on your server to a directory you configure in Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

For the device to recognize a new version is available, the firmware image must be downloaded from ExtremeNetworks.com to your server and saved in a directory you configure in Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **Options** tab.
2. Select **Inventory Manager** in the left panel.
3. Enter the **Firmware Directory Path** in either the FTP Server Properties, SCP Server Properties, or TFTP Properties section of the right panel, depending on the file transfer settings used.
4. Download the latest firmware image for your device from ExtremeNetworks.com and save it in the specified directory.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center server to the device.

1. Access the **Network** > **Firmware** tab.
2. Expand the **Device Type** navigation tree in the left-panel for the device family you are configuring and select the folder for the type of device.
3. Right-click the firmware file you downloaded (specified in the section above) and select **Set as Reference Image**.

NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality as well as provide bug fixes for existing features. Like firmware image upgrades, they are posted by Extreme Networks on github and ExtremeNetworks.com. Save XMODs in the directory you specify in the **Firmware Directory Path** field. Do not set an XMOD as the reference image.

IMPORTANT: ExtremeXOS devices on which version 21.1.1.4 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

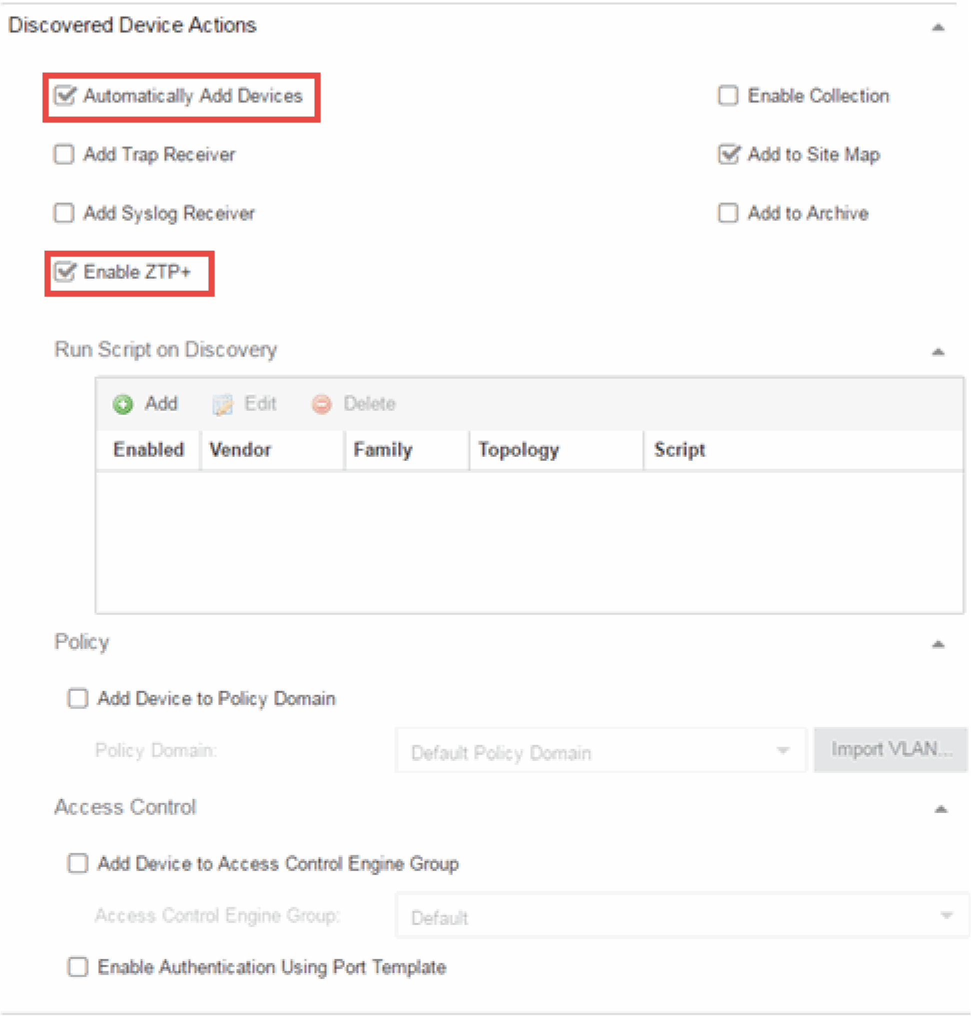
If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
2. Expand the World Site navigation tree and select the map in the left panel into which you are adding the devices.
3. Select the **Site** tab in the right panel.

4. Select the **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



Discovered Device Actions

☑ Automatically Add Devices
□ Enable Collection
□ Add Trap Receiver
☑ Add to Site Map
□ Add Syslog Receiver
□ Add to Archive
☑ Enable ZTP+

Run Script on Discovery

Enabled	Vendor	Family	Topology	Script

Policy

□ Add Device to Policy Domain

Policy Domain: Default Policy Domain

Access Control

□ Add Device to Access Control Engine Group

Access Control Engine Group: Default

□ Enable Authentication Using Port Template

5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.

8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

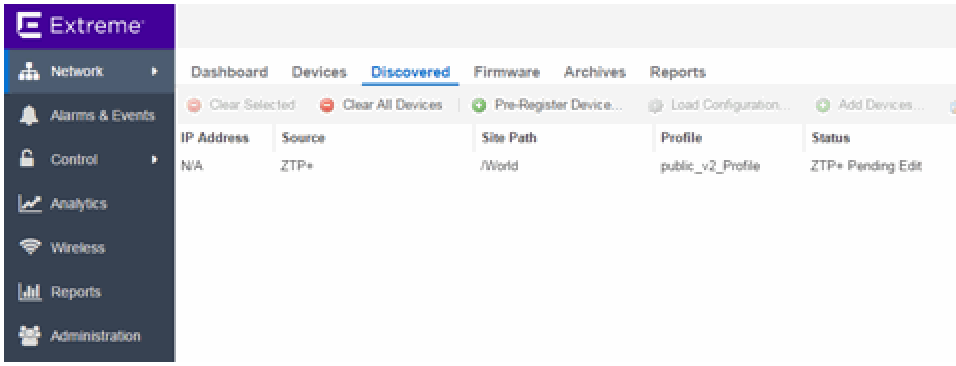
Adding the Device to the Extreme Management Center Database

Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the **Firmware** tab and set as Reference images, they are automatically installed.
2. Open the **Network** > **Discovered** tab in Extreme Management Center.

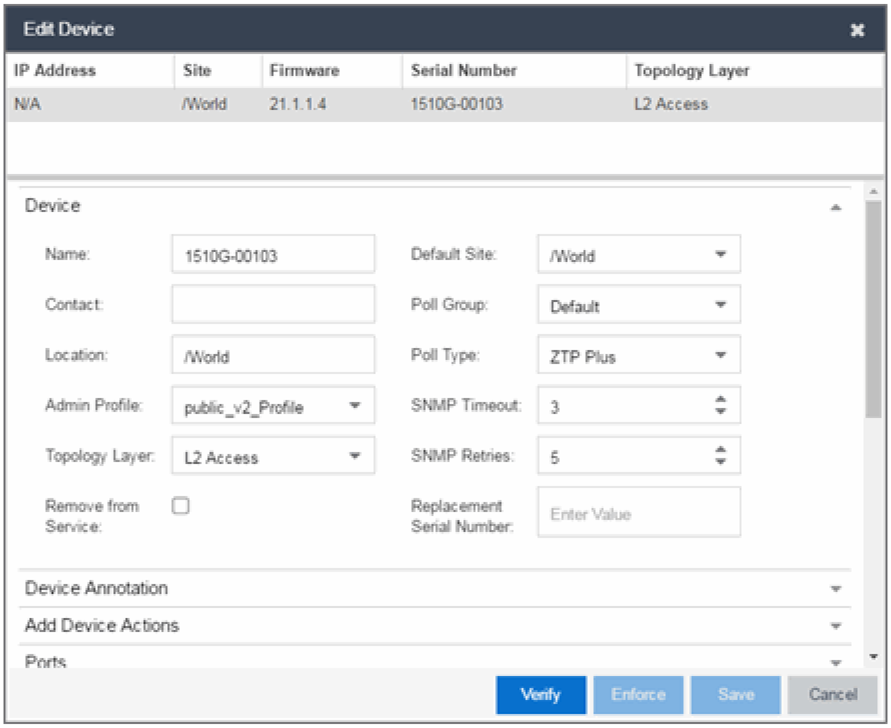
   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



IP Address	Source	Site Path	Profile	Status
N/A	ZTP+	/World	public_v2_Profile	ZTP+ Pending Edit

3. Select the device and click the **Edit Devices** button.

   The [**Edit Device** window] opens.



IP Address	Site	Firmware	Serial Number	Topology Layer
N/A	/World	21.1.1.4	1510G-00103	L2 Access

Name: 1510G-00103

Contact:

Location: /World

Admin Profile: public_v2_Profile

Topology Layer: L2 Access

Remove from Service: □

Default Site: /World

Poll Group: Default

Poll Type: ZTP Plus

SNMP Timeout: 3

SNMP Retries: 5

Replacement Serial Number: Enter Value

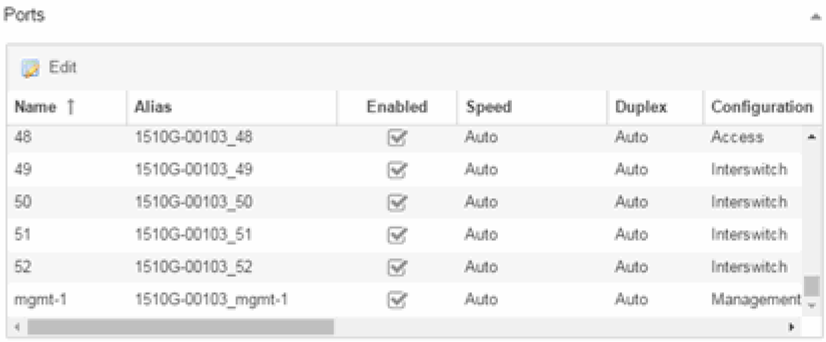
4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.

7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

> **NOTE:** Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.
10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.



Ports

Name ↑	Alias	Enabled	Speed	Duplex	Configuration
48	1510G-00103_48	☑	Auto	Auto	Access
49	1510G-00103_49	☑	Auto	Auto	Interswitch
50	1510G-00103_50	☑	Auto	Auto	Interswitch
51	1510G-00103_51	☑	Auto	Auto	Interswitch
52	1510G-00103_52	☑	Auto	Auto	Interswitch
mgmt-1	1510G-00103_mgmt-1	☑	Auto	Auto	Management

11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking the **Add** and **Delete** buttons, respectively.

    a. Enter the port **Alias**.

    b. Select the port **Configuration**, which is its role or purpose for the device.

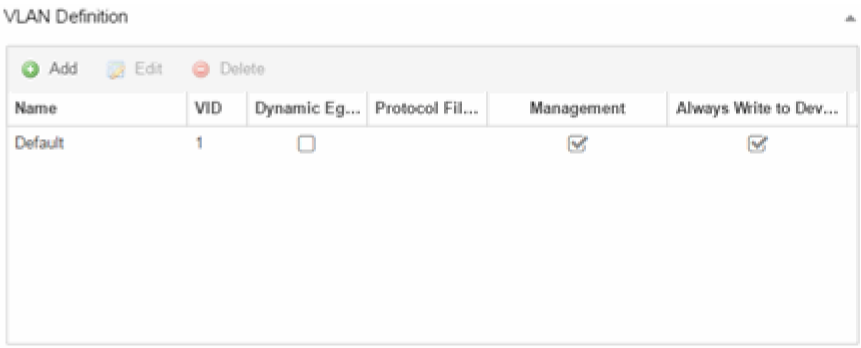
    - **Access** — The port provides access to end-systems.
    - **Interswitch** — The port connects the switch to another switch.
    - **Management** — The port is used to manage the network via Extreme Management Center.

    c. Enter a VLAN ID for the port in the **PVID** field.

    d. Configure the port **Speed** and **Duplex**.

12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



Name	VID	Dynamic Eg...	Protocol Fil...	Management	Always Write to Dev...
Default	1	□		☑	☑

13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the device remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the device, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the device resets and allows the process to restart.

The device **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Edit Device
- Devices

PortView

PortView is an Extreme Management Center component that provides port analysis and troubleshooting information including NetFlow data and Extreme Access Control end-system details, for your network wired and wireless devices.

The primary launch point for PortView is from the Extreme Management Center Search. Depending on the type of item you are searching for, one or more PortView tabs display with information pertaining to your search item. You can also launch PortView from other locations in Extreme Management Center, as well as in the legacy java applications Console and NAC Manager.

PortView lets you:

- View a topological display of device relationships.
- Analyze flow details, applications, senders, and receivers.
- Analyze real-time status, utilization, errors, and packets for a port.
- View the map of devices to which the end-system is connected.
- Analyze historical utilization and availability for a port.
- View all end-systems attached to a port and critical end-system information.

This Help topic provides the following PortView information:

- Requirements
    - License and Data Collection Requirements
    - Access Requirements
- Launching PortView
    - Launching from Extreme Management Center
    - Launching from Console
    - Launching from NAC Manager

Requirements

License and Data Collection Requirements

You must have a Extreme Management Center license (NMS) or Extreme Management Center Advanced license (NMS-ADV) to view PortView reports. (Contact your sales representative for information on obtaining Extreme Management Center licenses.)

In addition, the information provided in each report depends on the selected switch and the report data collections you configure. For information on configuring data collection, see Enable Report Data Collection.

The following chart describes the complete set of PortView reports and provides the data collection requirements for each report (if applicable). Some of these reports are available as PortView tabs, others are launched from the right-click menu in the graphical Overview report.

PortView Report	Description	Requirements
Overview	Topological display of device relationships.	
Application Summary	View reports that present a summary of application information.	
Details	The tabs within the report contain the following information: Access Profile — Displays an interactive fingerprint containing information about the end-system. Click an icon to open additional details. End-System — View information about the end-system. End-System Events — View the Extreme Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. Health Results — Displays risk information for the selected end-system.	Switch must have Extreme Access Control authentication enabled.
Map	Displays the map containing the device to which the end-system is connected.	
Sessions	The tabs within the report contain the following information: Interface History — Historical interface utilization and availability. Client History — Historical statistics for wired or wireless clients. End-System Events — View the Extreme Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. NetFlow — NetFlow data for the selected port.	Requires active interface statistics collection. Client statistics collection must be enabled. Switch must have Extreme Access Control authentication enabled. The switch must support NetFlow and flow collection must be enabled on the port.

PortView Report	Description	Requirements
Network Information	The tabs within the report contain the following information: Wireless Details — Presents controller, AP, or client information, depending on your search. Interface Details — Real-time interface status, utilization, and errors. AP History — Contains historical data for your APs. Switch Resources — Switch CPU and memory utilization statistics. Device Resources — Device CPU and memory utilization statistics.	Requires active device statistics collection. Requires active device statistics collection.

Access Requirements

Access to PortView reports is determined by the user's membership in a Extreme Management Center authorization group and the group's assigned capabilities. The following table lists the capabilities required for access to the different PortView reports. For more information on how to configure capabilities and authorization group membership, see the Help topic "How to Configure User Access to Extreme Management Center Applications" located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

PortView Report	Required Capability
Network Information Interface History Client History Client Event History Switch History Controller History	NetSight OneView > Access OneView or NetSight OneView > Access OneView and Access OneView Administration
Sessions > NetFlow	NetSight OneView > NetFlow Read Access
Modify Flow Collection	NetSight OneView > NetFlow Read/Write Access
Map	NetSight OneView > Maps > Maps Read Access or Maps Read/Write Access
Details Sessions > End-System Events	NetSight OneView > Extreme Access Control > OneView End-Systems Read Access or NetSight OneView > Extreme Access Control > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in Extreme Management Center, as well as the legacy java applications Console and NAC Manager. By default, you can have five active PortView searches displayed in Extreme Management Center at one time. You can change this display limit in the **Maximum PortViews Displayable** field in Management Center Options (Administration > Options > Management Center > Session Limits).

NOTE: A single PortView search returns a maximum of five matching results. If the number of matching results exceeds five, an error message appears asking you to refine the search term and try again.

Launching from Extreme Management Center

Extreme Management Center Search Tab

The primary launch point for PortView is from Extreme Management Center Search. The Search page provides a search field where you can enter a MAC address, IP address, host name, AP serial number, or Extreme Access Control custom field information to begin searching. Depending on the type of item for which you are searching, the search results return one or more PortView tabs, with information pertaining to your search item. You can right-click on the different devices in the topology results to launch additional reports.

1. Open the **Search** tab.
2. Enter a MAC address, IP address, host name, AP serial number, or Identity and Access custom field information, and press **Enter** to begin the search. You can copy the IP or MAC address from another source and enter it into the **Search** field. For example, you can copy an end-system MAC address from the **Control** tab End-Systems view, and then paste the MAC address into the search field and press **Enter**.
3. Depending on the type of item for which you are searching, the secondary navigation bar displays one or more PortView tabs, with information pertaining to your search item, similar to the search results shown below.

Extreme Management Center Interface Summary FlexView

Use the following steps to launch PortView from a Extreme Management Center Interface Summary FlexView.

1. On the **Network** tab, click on the device Name link to open the Interface Summary FlexView.
2. In the Interface Summary, click on the interface Name or Alias link to open PortView.

Launching from Console

You can launch PortView from Console using any of the following methods:

- In the **Port Properties** tab, right-click on one or more ports and select **Port Tools** > **PortView**.

- In the Compass Results table, right-click on up to four entries and select **Port Tools** > **PortView**.
- In the Interface Summary FlexView, right-click on one or more ports and select **Port Tools** > **PortView**.

Launching from NAC Manager

You can launch the PortView Extreme Access Control reports from NAC Manager using either of the following two methods:

- In the **End-Systems** tab, right-click on an end-system in the table and select **PortView** from the menu.
- On the **Control** tab's End-Systems view, right-click the entry with the desired switch port and select **PortView** from the menu.

AP Wireless Real Capture

Real Capture allows real-time collection of Access Point (AP) wireless traffic for troubleshooting and problem resolution. Real Capture collects traces on the AP wireless interface and transmits them to Wireshark running on a local Windows client. It allows Wireshark to capture RF/wireless traffic as if it were running directly on the AP, providing visibility into network connectivity and performance issues. All Wireshark features are supported, including filters and I/O graphs.

NOTE: APs must be running firmware version 8.x or later. The AP2600 series of Access Points does not support the Real Capture feature.

Real Capture can be enabled for each AP individually from PortView in the Extreme Management Center. When it is enabled, Real Capture runs a daemon on the AP that allows it to interface with Wireshark using port 2002 or 2003. The AP then captures all the wireless traffic (except for management traffic) originating from the AP and sends it to Wireshark for analysis.

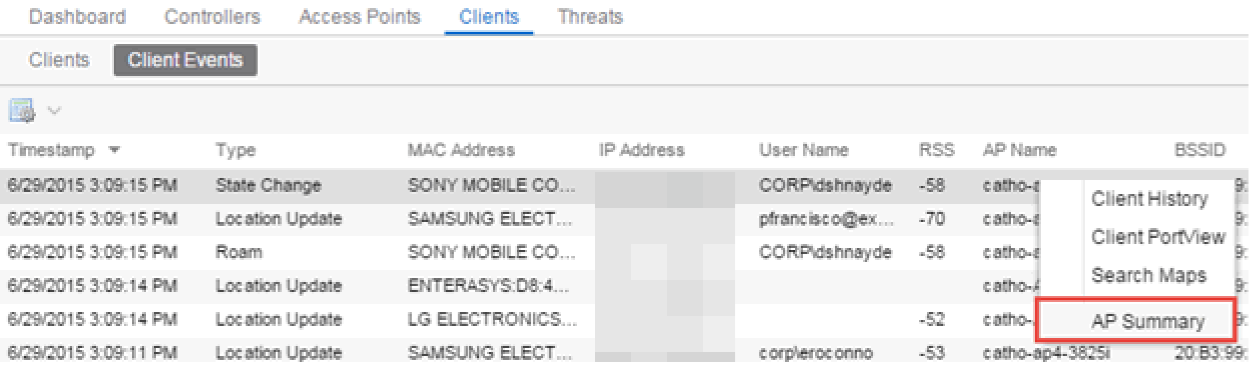
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing the 802.11n preamble header using the AP CLI commands.

NOTE: When capturing client traffic on the AP, if the topology is bridged at AP, client traffic is captured and can be analyzed in the resultant trace. However, if the topology is bridged at controller, only WASSP traffic is captured as the AP tunnels this communication back to the controller. This traffic must be sent to the Extreme Networks Support for analysis because it needs to be decoded. In this scenario, it may be better to mirror the switch port where the controller connects to the LAN.

Configure and Use Real Capture

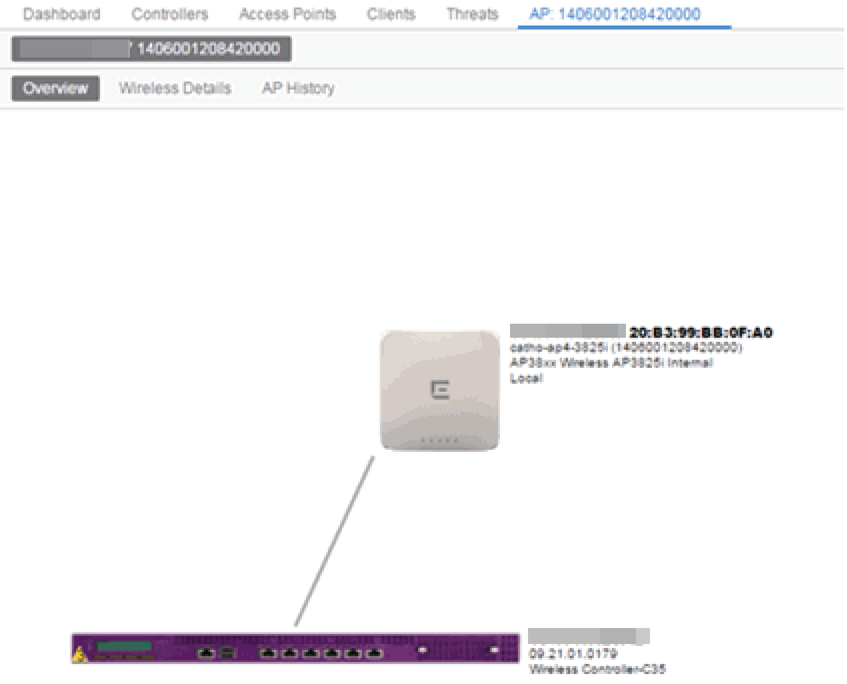
Use the following steps to configure and use the Real Capture feature.

1. Launch Extreme Management Center.
2. Launch PortView for the AP from the Wireless Client Event History report.
   a. Select the **Wireless** tab and then select the **Clients** tab and the **Client Events** sub-tab. Right-click on the AP Name and select **AP Summary** from the menu.



Timestamp ▾	Type	MAC Address	IP Address	User Name	RSS	AP Name	BSSID
6/29/2015 3:09:15 PM	State Change	SONY MOBILE CO...	[redacted]	CORP\dshnayde	-58	catho-a	9:
6/29/2015 3:09:15 PM	Location Update	SAMSUNG ELECT...	[redacted]	pfrancisco@ex...	-70	catho-a	9:
6/29/2015 3:09:15 PM	Roam	SONY MOBILE CO...	[redacted]	CORP\dshnayde	-58	catho-a	9:
6/29/2015 3:09:14 PM	Location Update	ENTERASYS:D8:4...	[redacted]			catho-A	9:
6/29/2015 3:09:14 PM	Location Update	LG ELECTRONICS...	[redacted]		-52	catho-	9:
6/29/2015 3:09:11 PM	Location Update	SAMSUNG ELECT...	[redacted]	corp\eroconno	-53	catho-ap4-3825i	20:B3:99:

   b. The AP PortView opens.



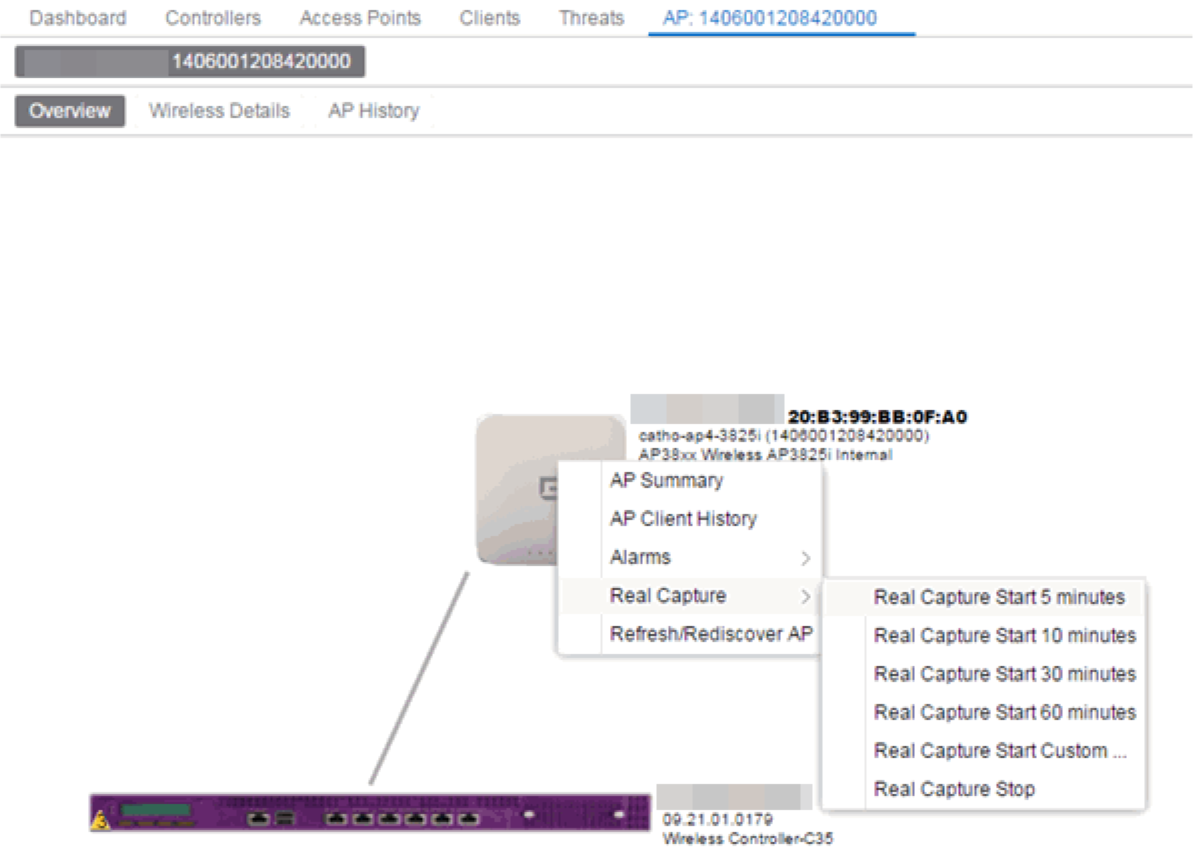
[redacted] 1406001208420000

[redacted] 20:B3:99:BB:0F:A0
catho-ap4-3825i (1406001208420000)
AP38xx Wireless AP3825i Internal
Local

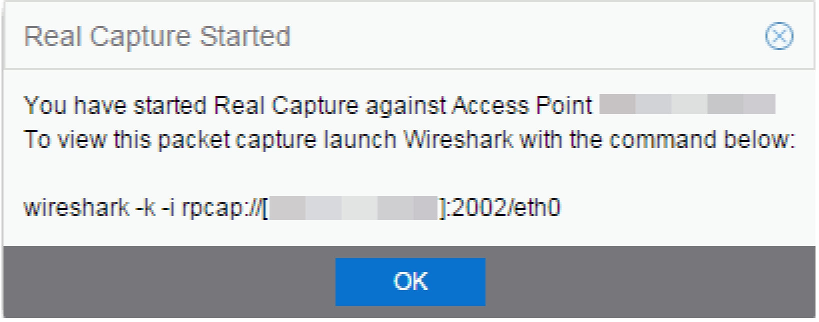
[redacted]
09.21.01.0179
Wireless Controller-C35

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**.


Dashboard
Controllers
Access Points
Clients
Threats
AP: 1406001208420000
[redacted] 1406001208420000
Overview
Wireless Details
AP History
[redacted] 20:B3:99:BB:0F:A0
catho-ap4-3825i (1406001208420000)
AP38xx Wireless AP3825i Internal
AP Summary
AP Client History
Alarms
Real Capture
Refresh/Rediscover AP
Real Capture Start 5 minutes
Real Capture Start 10 minutes
Real Capture Start 30 minutes
Real Capture Start 60 minutes
Real Capture Start Custom ...
Real Capture Stop
[redacted]
09.21.01.0179
Wireless Controller-C35

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.



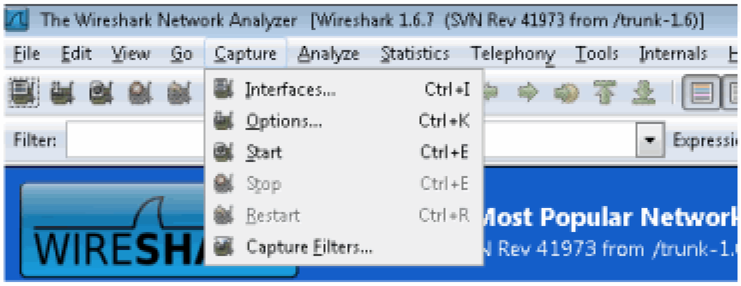
Real Capture Started

You have started Real Capture against Access Point [redacted]
To view this packet capture launch Wireshark with the command below:

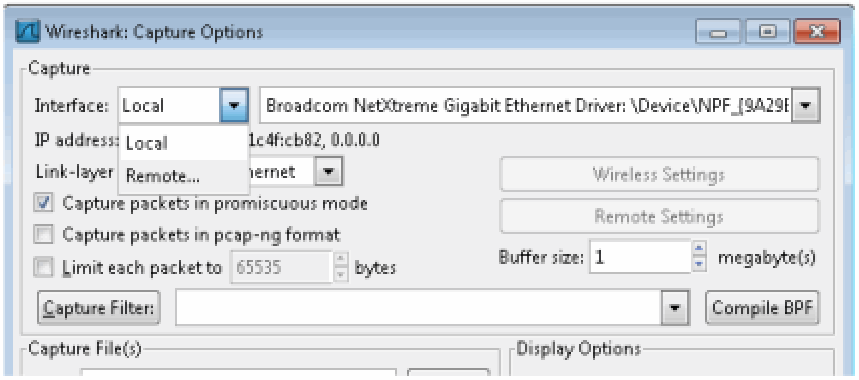
```
wireshark -k -i rpcap://[[redacted]]:2002/eth0
```

5. You can also access the captured traffic in Wireshark using the following steps:

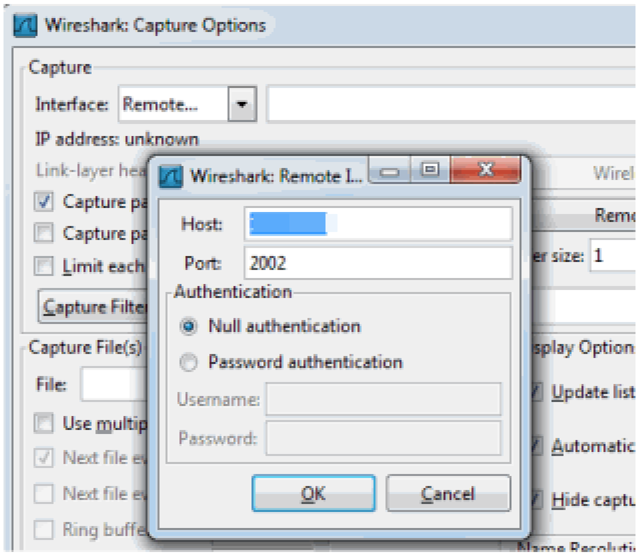
   a. In Wireshark, select **Capture** > **Options** from the menu bar.



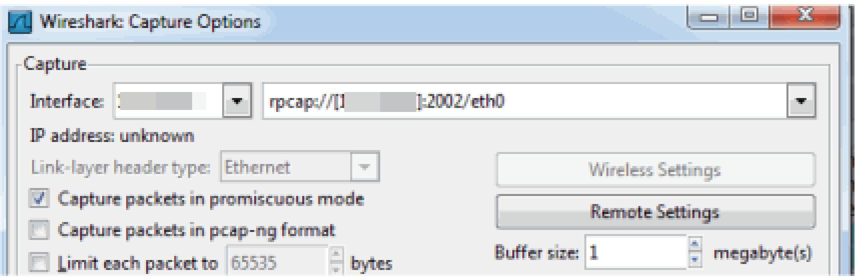
   b. In the Capture Options window, set the **Interface** value to **Remote**.


Wireshark: Capture Options
Capture
Interface: Local
Broadcom NetXtreme Gigabit Ethernet Driver: \Device\NPF_{9A29E
IP address: Local
1c4f:cb82, 0.0.0.0
Link-layer Remote...
ernet
Wireless Settings
Remote Settings
☑ Capture packets in promiscuous mode
☐ Capture packets in pcap-ng format
☐ Limit each packet to 65535 bytes
Buffer size: 1 megabyte(s)
Capture Filter:
Compile BPF
Capture File(s)
Display Options

   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.



Wireshark: Capture Options

Capture

Interface: [redacted] rpcap://[[redacted]]:2002/eth0

IP address: unknown

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

□ Capture packets in pcap-ng format

□ Limit each packet to 65535 bytes

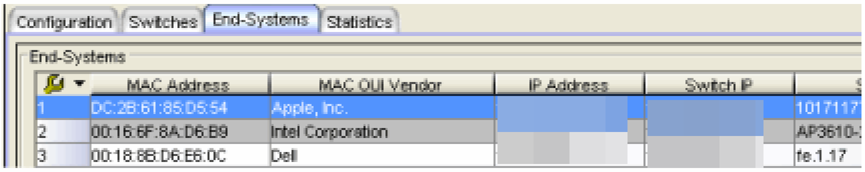
Buffer size: 1 megabyte(s)

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.

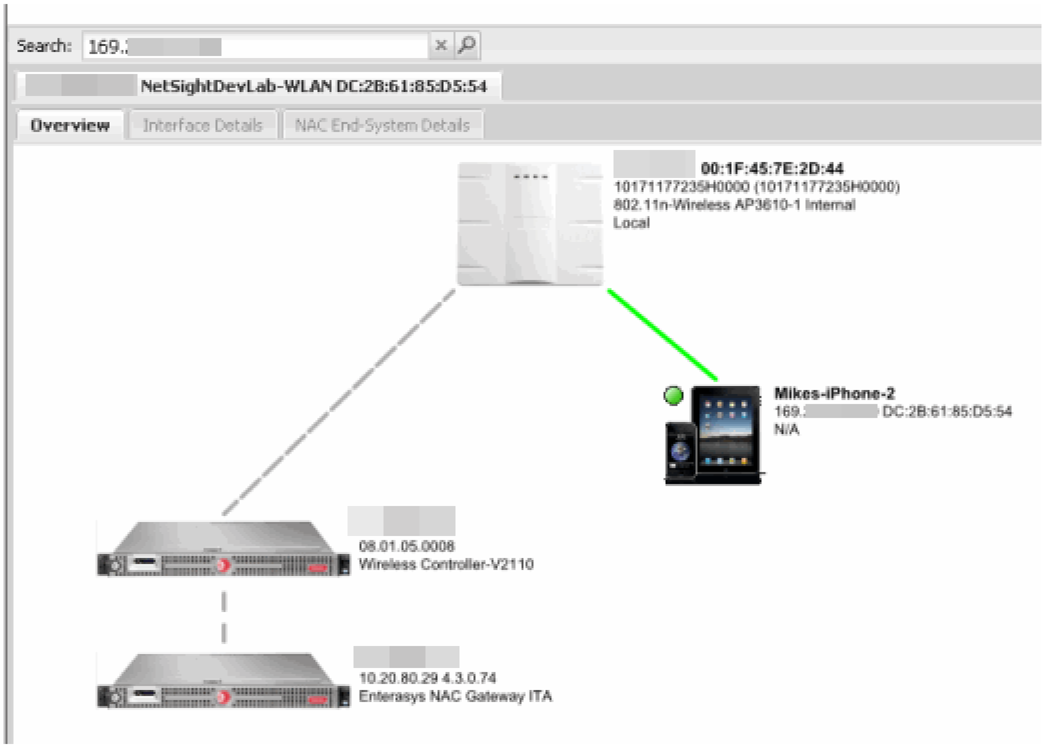
The problem starts when an end-system in NAC Manager is not able to obtain an IP address.



End-Systems

	MAC Address	MAC OUI Vendor	IP Address	Switch IP	S
1	DC:2B:61:85:D5:54	Apple, Inc.	[redacted]	[redacted]	1017117
2	00:16:6F:8A:D6:B9	Intel Corporation	[redacted]	[redacted]	AP3610-
3	00:18:8B:D6:E6:0C	Dell	[redacted]	[redacted]	fe.1.17

A search is performed on the 169.x.x.x IP address.



Search: 169.[redacted]

[redacted] NetSightDevLab-WLAN DC:2B:61:85:D5:54

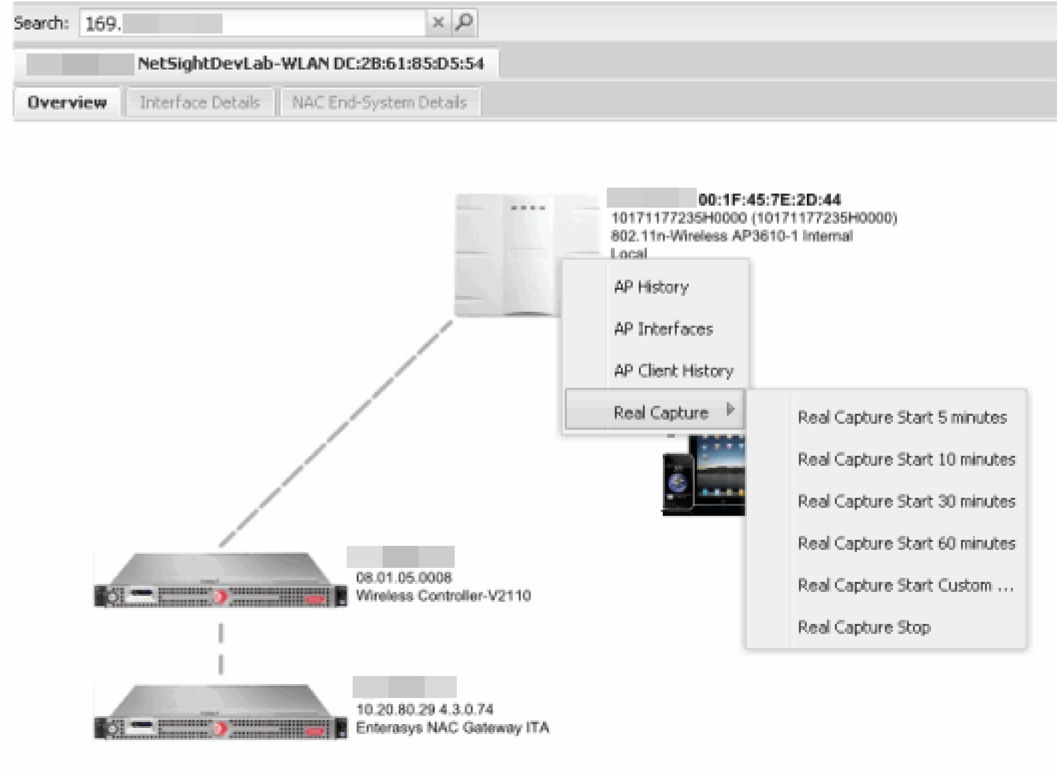
[redacted] 00:1F:45:7E:2D:44
10171177235H0000 (10171177235H0000)
802.11n-Wireless AP3610-1 Internal
Local

Mikes-iPhone-2
169.[redacted] DC:2B:61:85:D5:54
N/A

[redacted]
08.01.05.0008
Wireless Controller-V2110

[redacted]
10.20.80.29 4.3.0.74
Enterasys NAC Gateway ITA

The traffic capture is started on the AP to which the end-system is connected.



Search: 169.[redacted]

[redacted] NetSightDevLab-WLAN DC:2B:61:85:D5:54

Overview
Interface Details
NAC End-System Details

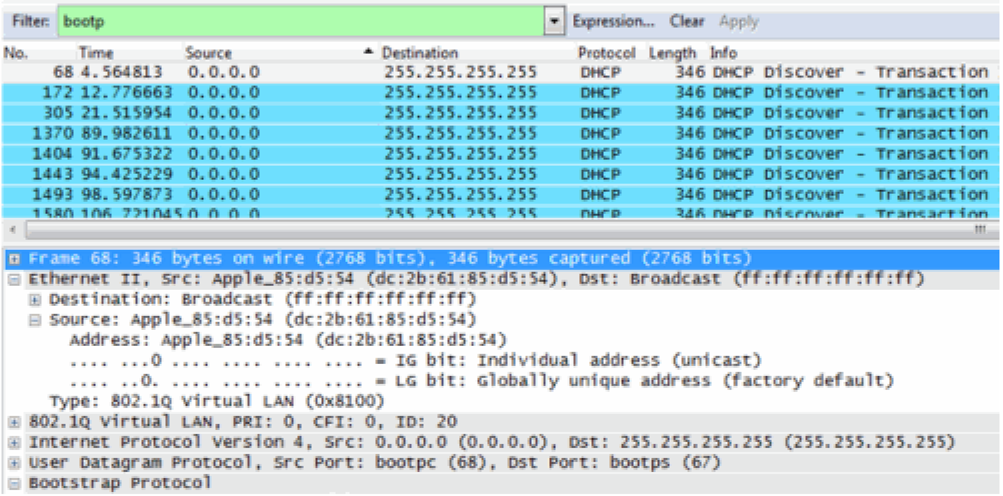
[redacted] 00:1F:45:7E:2D:44
10171177235H0000 (10171177235H0000)
802.11n-Wireless AP3610-1 Internal
Local

AP History
AP Interfaces
AP Client History
Real Capture
Real Capture Start 5 minutes
Real Capture Start 10 minutes
Real Capture Start 30 minutes
Real Capture Start 60 minutes
Real Capture Start Custom ...
Real Capture Stop

[redacted]
08.01.05.0008
Wireless Controller-V2110

[redacted]
10.20.80.29 4.3.0.74
Enterasys NAC Gateway ITA

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.



```
No.     Time        Source          Destination       Protocol Length Info
     68 4.564813    0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
    172 12.776663   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
    305 21.515954   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
   1370 89.982611   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
   1404 91.675322   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
   1443 94.425229   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
   1493 98.597873   0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction
   1580 106.721045  0.0.0.0         255.255.255.255   DHCP        346 DHCP Discover - Transaction

⊞ Frame 68: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
⊟ Ethernet II, Src: Apple_85:d5:54 (dc:2b:61:85:d5:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Source: Apple_85:d5:54 (dc:2b:61:85:d5:54)
      Address: Apple_85:d5:54 (dc:2b:61:85:d5:54)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: 802.1Q Virtual LAN (0x8100)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
```

How to Use the Report Designer

The Report Designer lets you create custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The Report Designer also lets you create a new report based on individually selected components. Once a report is created, it is available from the report catalog in the Reports tab.

The Report Designer can be accessed from the Reports tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

This Help topic provides the following information:

- Creating a Report
- Modifying a Report
- Deleting a Report
- Custom Components

Creating a Report

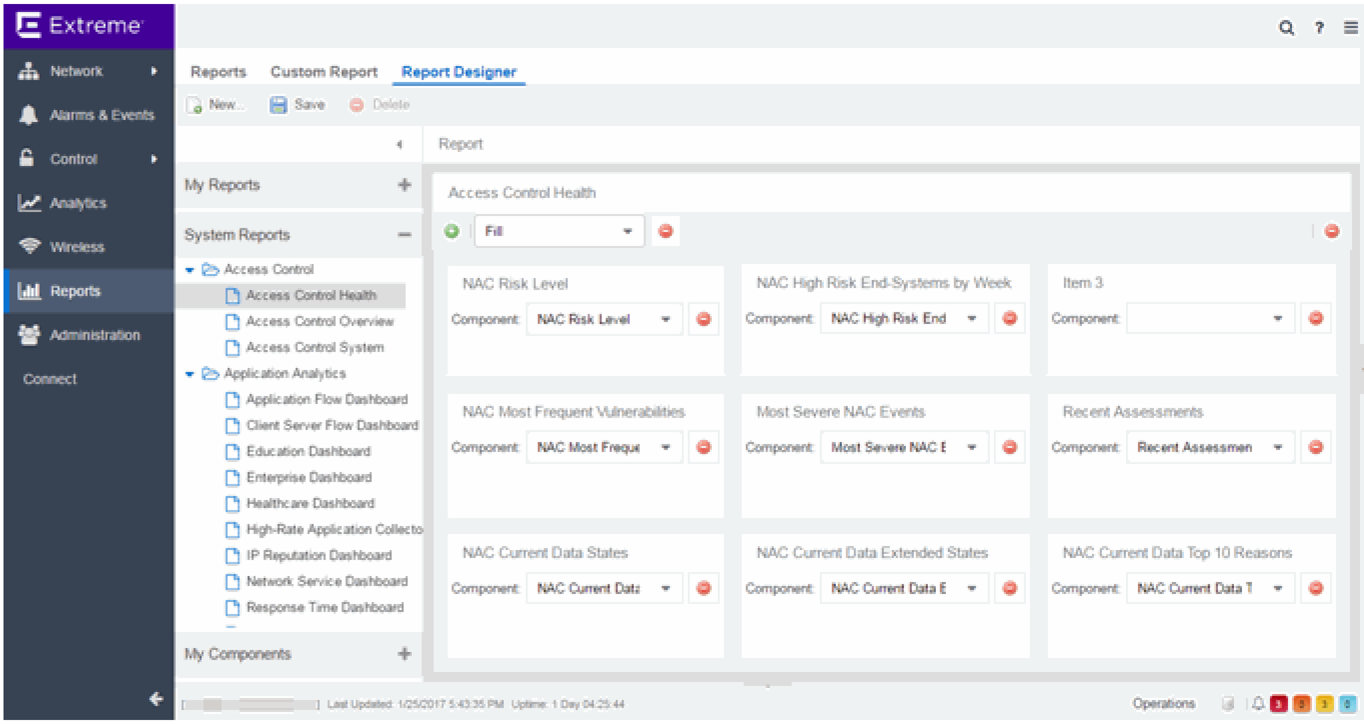
There are two ways to create a report. You can create a report by customizing an existing dashboard report (system report) or by creating a new report based on a selection of individual components.

Customize a System Report

Use the following steps to customize an existing system report. The customized report replaces the original report in the **Reports** tab and all other places in Extreme Management Center where that report is used.

For example, you want to delete some of the dashboard panels and change some of the dashboard components in the Extreme Access Control System report.

1. Select the **Reports** tab in Extreme Management Center and then select the **Report Designer**.
2. Select the system report you want to customize in the System Reports section. In the example below, Extreme Access Control > Extreme Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



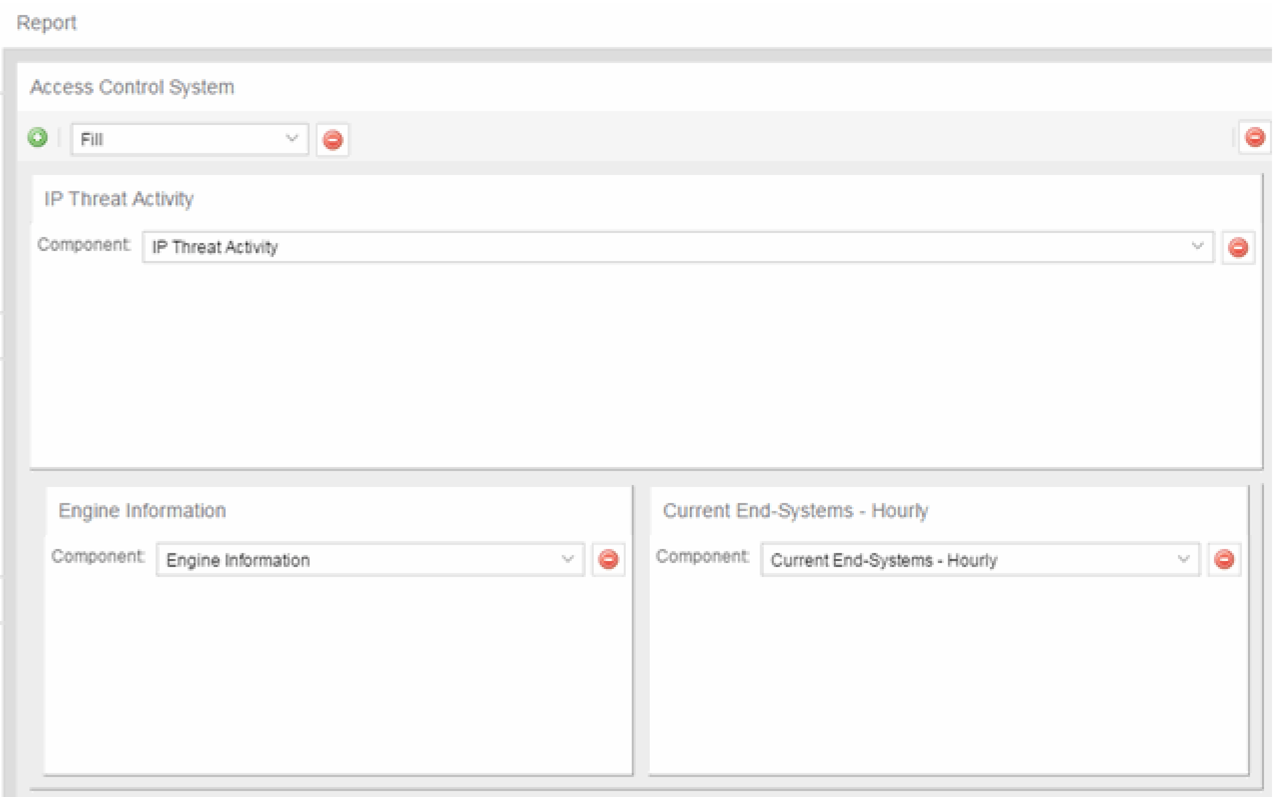
Access Control Health

Fill

NAC Risk Level Component: NAC Risk Level	NAC High Risk End-Systems by Week Component: NAC High Risk End	Item 3 Component:
NAC Most Frequent Vulnerabilities Component: NAC Most Freque	Most Severe NAC Events Component: Most Severe NAC E	Recent Assessments Component: Recent Assessmen
NAC Current Data States Component: NAC Current Data	NAC Current Data Extended States Component: NAC Current Data E	NAC Current Data Top 10 Reasons Component: NAC Current Data T

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.



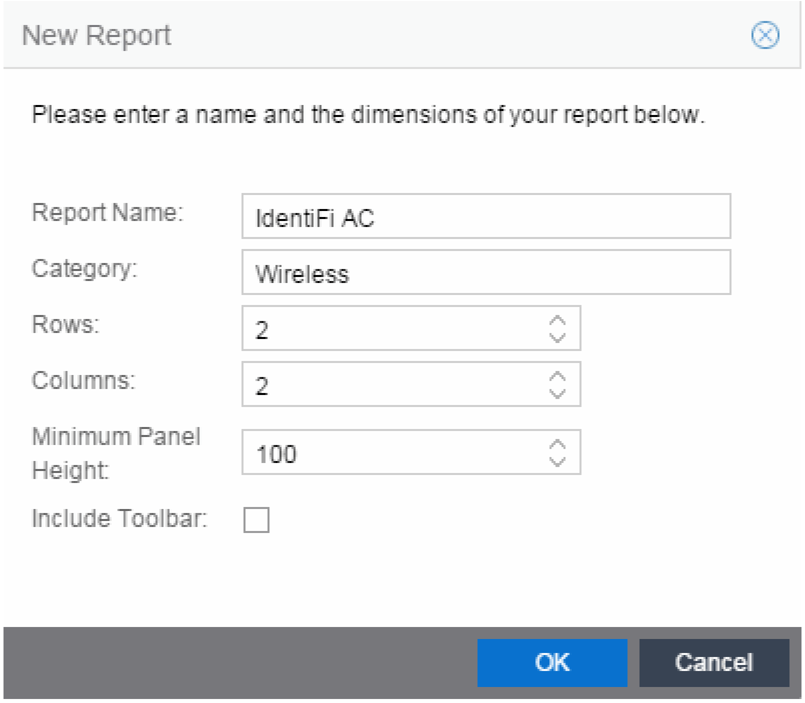
4. Once you have finished making changes to the report, click the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

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.



New Report

Please enter a name and the dimensions of your report below.

Report Name: IdentiFi AC

Category: Wireless

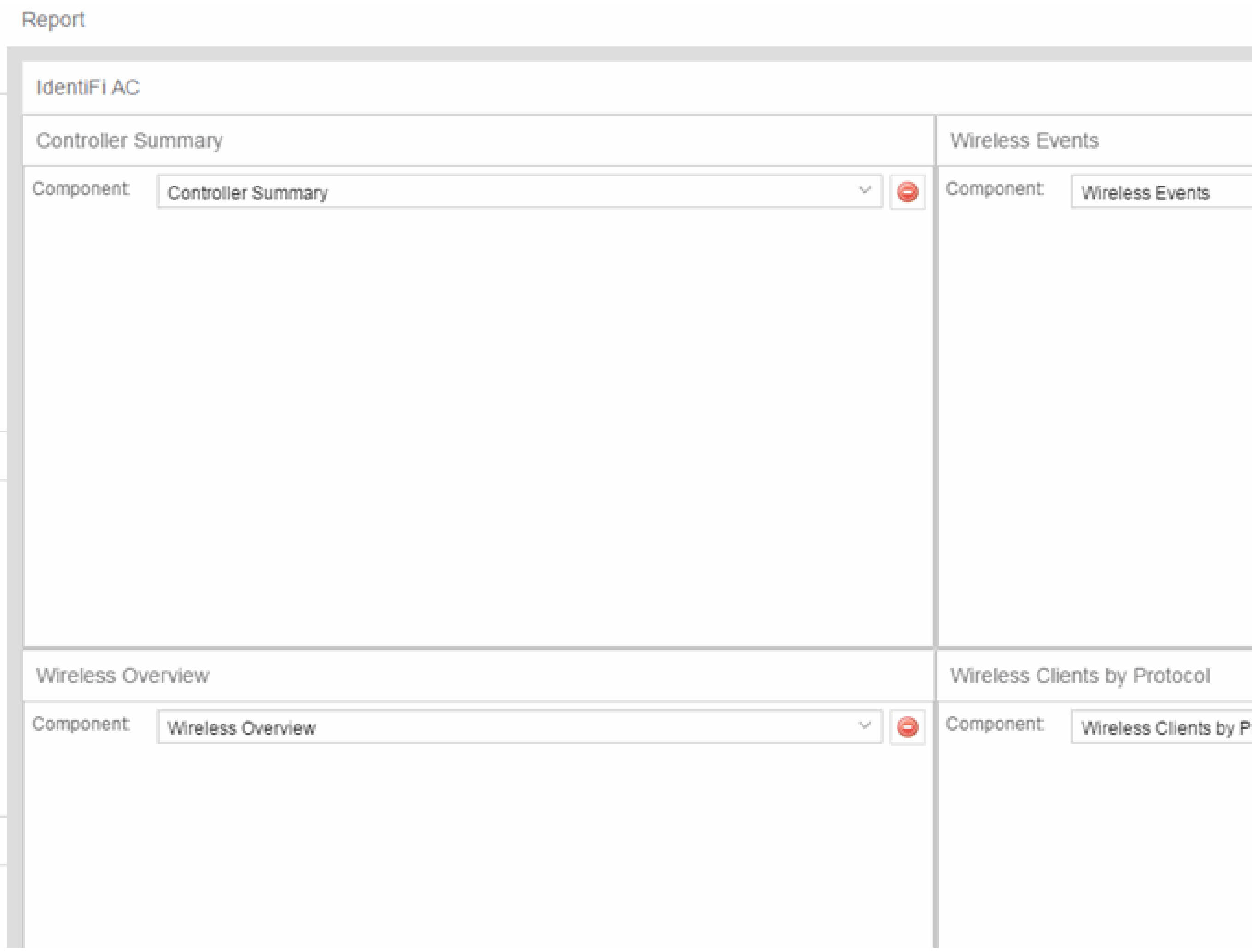
Rows: 2

Columns: 2

Minimum Panel Height: 100

Include Toolbar: □

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.


Report

IdentiFi AC

Controller Summary

Component: Controller Summary

Wireless Events

Component: Wireless Events

Wireless Overview

Component: Wireless Overview

Wireless Clients by Protocol

Component: Wireless Clients by P

9. Click the **Save** button. The report populates with data and displays in a new tab as a way to preview the report.

The new report is now listed in the **Reports** tab under the appropriate category.

Modifying a Report

You can change a report's components and delete panels, but you cannot add new panels. If you want to add new panels, you must create a new report.

1. Select the **Reports** tab and then select the **Report Designer**.
2. In the My Reports section, select the report you want to modify. The report displays in the right panel for editing.

3. Use the **Component** drop-down menu to change a component in a panel, or click the **Delete** button to delete a panel.
4. Click the **Save** button. The report populates with data and displays in a new tab. This allows you to preview how the customized report looks.

The new report is now listed in the **Reports** tab under the appropriate category.

Deleting a Report

You can delete a customized system report from the My Reports section in the Report Designer. This also deletes the customized report from the **Reports** tab, and replaces it with the original system report. The original report is available again from the System Reports section in the Report Designer.

You can delete a new report from the My Reports section in the Report Designer. This also deletes the new report from the **Reports** tab.

Custom Components

When you create an Advanced Browser report in the Application Analytics Browser, you can save it to the Report Designer to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section of the Report Designer. They are available for selection from the **Component** drop-down menu in the Applications Browser section when you customize a system report or create a new report.

Related Information

For information on related topics:

- Reports

How to Create a New Report Using the Report Designer

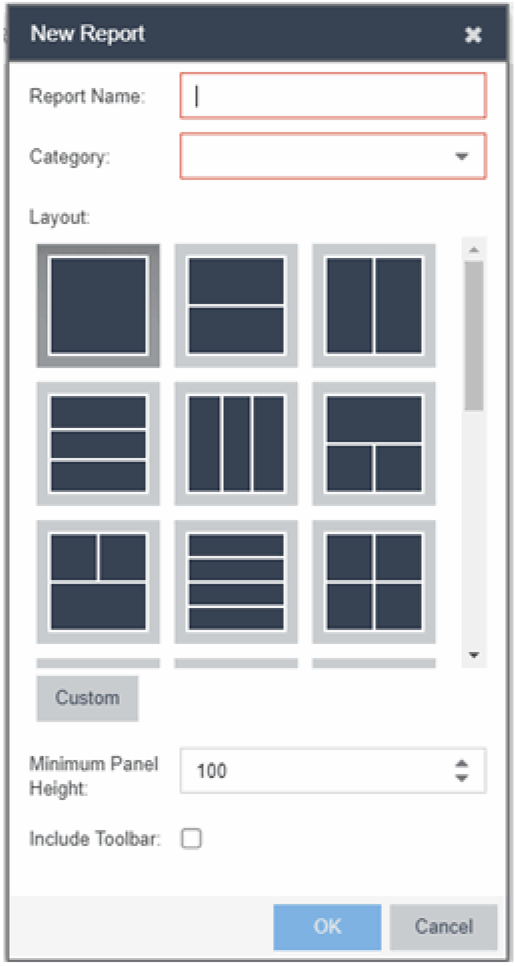
The Report Designer lets you create custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The Report Designer can be accessed from the **Reports** tab. The Report Designer also lets you create a new report based on individually selected components. Once a report is created, it is available from the report catalog in the **Reports** tab.

In order to use the Report Designer, you must be a member of an authorization group that is assigned the Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

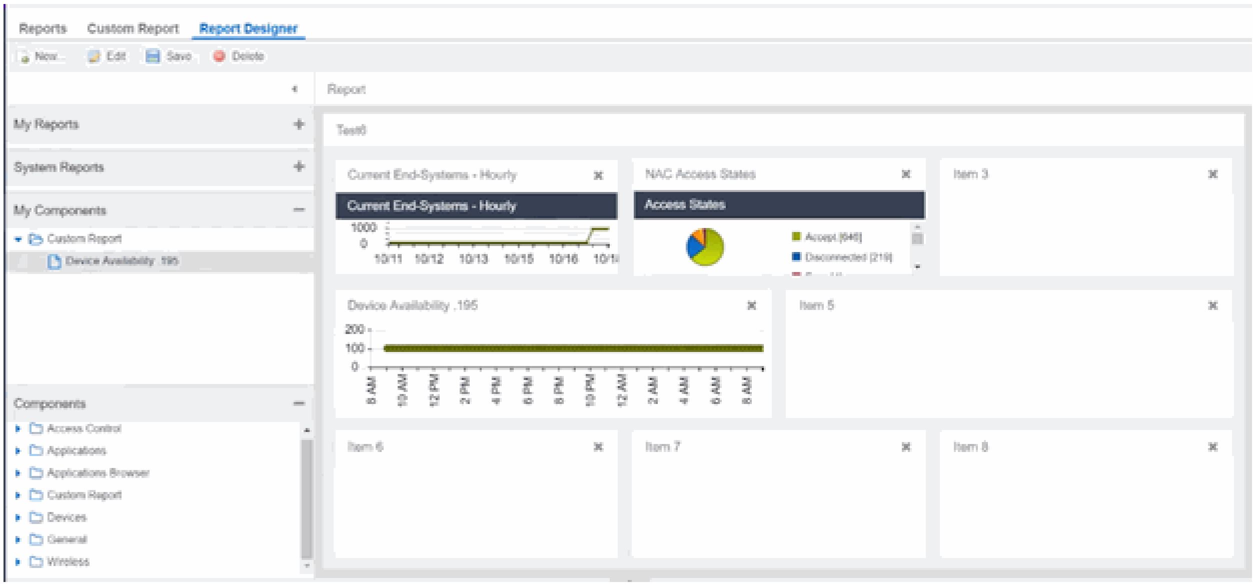
Creating a New Report

Use the following steps to create a new report. The new report is added to the **Reports** tab.

1. Select the **Reports > Report Designer** tab.
2. Click on the **New** button. The New Report window opens. Use this window to define the report characteristics.



3. Enter a **Report Name**. Use an easy to recognize name in the **Reports** tab.
4. Select a **Category** for the report from the drop-down menu or enter a category in the Category box. This allows you to group your report within an existing report category (in the **Reports** tab) or create a new category.
5. Select from the **Layout** options to determine the number of reports that are displayed in each row and column of your dashboard.
6. Select the **Minimum Panel Height** from the drop-down menu.
7. Click the **Include Toolbar** box to add the tool bar to your dashboard.
8. Click the **OK** button. The empty layout format displays in a new tab.
9. Drag and drop the components from the left panel that you want displayed in the dashboard.
10. Once in place, the components are a live preview of the data.



11. Click **Save**. The new report is now listed in the **Reports** tab under the appropriate category.

Related Information

- ExtremeAnalyticstab

How to Customize a Report Using the Report Designer

The Report Designer lets you create custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The **Report Designer** also lets you create a new report based on individually selected components. Once a report is created, it is available from the report catalog in the Reports tab.

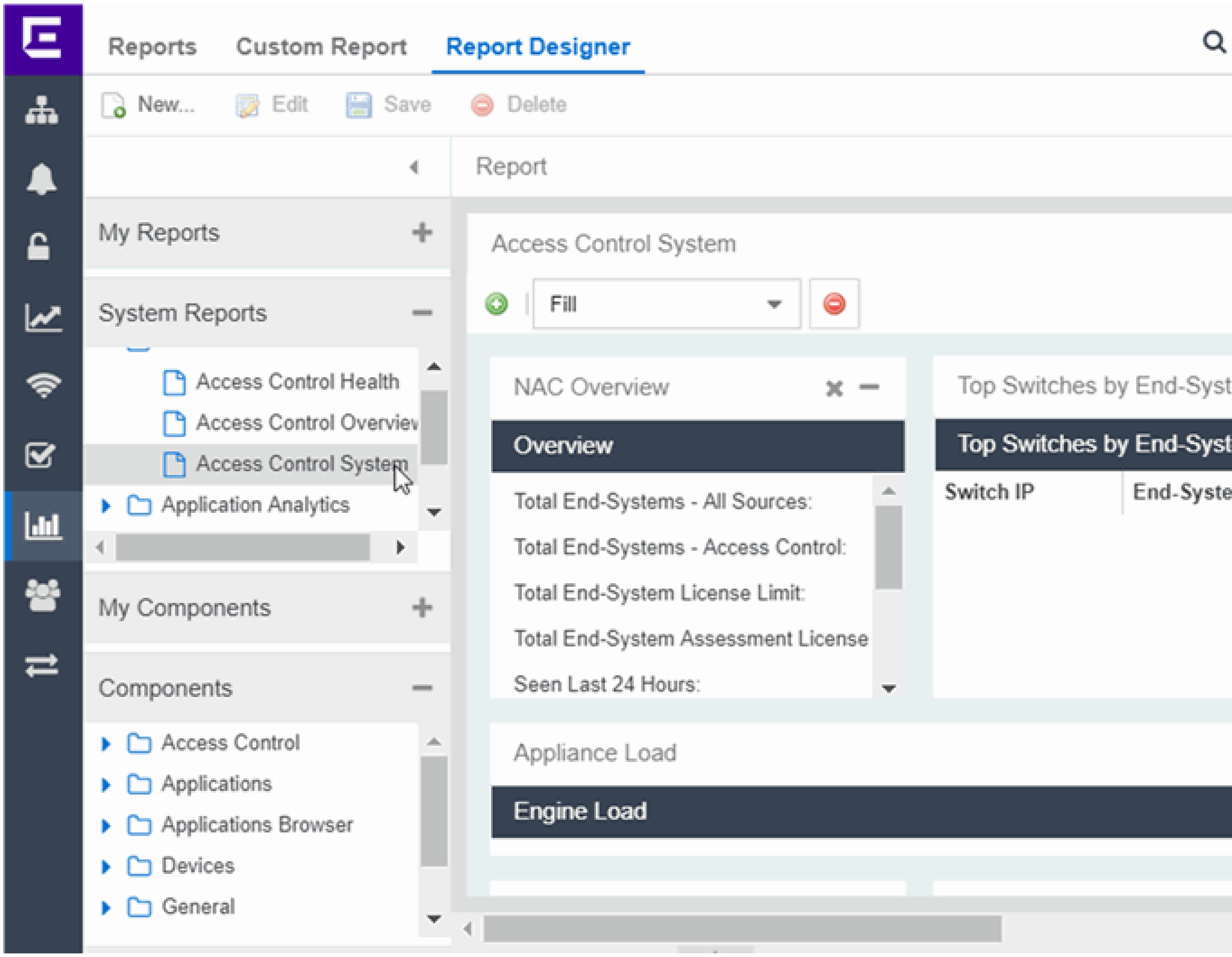
The Report Designer can be accessed from the **Reports** tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

Customizing a System Report

Use the following steps to customize an existing system report. The customized report replaces the original report in the **Reports** tab and all other places in Extreme Management Center where that report is used.

For example, you want to delete some of the dashboard panels and change some of the dashboard components in the Extreme Access Control System report.

1. Select the **Reports** tab in Extreme Management Center and then select the **Report Designer**.
2. Select the system report you want to customize in the System Reports section. In the example below, Extreme Access Control > Extreme Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
    a. Drag and drop the components that you want displayed in the dashboard.
    b. Once in place, the components are a live preview of the data.
4. Once you have finished making changes to the report, click the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

The custom system report is available in the Reports catalog and replaces the original system report. If you delete the customized system report, the report changes back to the original system report.

Related Information

- Reports Catalog

Reports Catalog

Extreme Management CenterReports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

Select from a catalog of reports, many of which are interactive, allowing you to adjust the data and time on which to report. See below for a description of each report and a section on helpful report features and functionality. Use the **Info** button ℹ at the top-right of the Extreme Management Center page to access detailed information about many of the reports.

Reports Catalog

The Reports catalog lets you select a report from the following report types:

- Extreme Access Control — Provides an overview of end-system connection information. You can also see these reports and others on the **Control** tab.
- Extreme Access Control Health — Provides reports on end-system assessment and state information. In the Risk Level pie chart, click on a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.
- Extreme Access Control System — Provides a report of the top ten end-systems by engine.
- Application Analytics — These reports provide visibility into the applications on your network and who's using those applications.
- Console — The NMS Dashboard report provides summary NMS data including top 5 switch, interface, and host statistics as well as important Wireless data. Host data is collected from network devices that support the Host Resource MIB, such as Extreme Management Center engines, Linux systems, and Windows PCs. For more information, click the **Info** button (ℹ) at the top-right of the **Reports** tab.
- Data Center Manager — The DCM reports provide an overview of all virtual machines on the network broken down into VM distribution per Identity and Access profile, Operating System, Switch, and Hypervisor technology. They also provide table reports with detailed information on all VMs. For each supported Hypervisor technology, sub-reports provide more in-depth data.

- Device — The Device reports provide information on device alarms, device archives (archive events and details), device availability, down devices, inventory summary (including archive distribution, devices backed up, database properties, scheduled events, asset tracking information, and the ability to track the changes made to a specific device), top devices by IPv6 traffic, top hosts by resource (memory, CPU, and disk usage), top switches by power (percent usage and consumption in watts), and top switches by resource (CPU and physical memory).
- Interface — These reports present information on your top interfaces by active flows, bandwidth, bandwidth summary, least availability, POE usage, and utilization.
- OpenScape — The OpenScape LIA (Location and Identity Assurance) report provides an overview of all OpenScape phones on the network categorized by phone count, phone type, phone software version, and phone distribution by access switch, as well as a list of phone information by MAC address.
- Policy — Provides a policy rule hit summary report showing top services and roles by rule hits.
- Server — These reports provide data on the Extreme Management Center server, including the Event Log, CPU and heap memory utilization, and disk access information. The information in the Console Event Log report is the same as the Alarms and Events tab. For more information on using this report, see the "Alarms and Events" Help topic.
- Wireless — A collection of summary reports providing information on your wireless network components, including reports for AP groups, APs, clients, controllers, and mobility zones. Wireless reports also provide data on wireless components ranked by bandwidth and clients, such as top APs by bandwidth, top clients by bandwidth, and top controllers by clients, as well as reports on APs and controllers that are down. For convenience, you can also view some of these reports from the Wireless tab.
- PDF Reports — Generate summary reports of your current network configuration in PDF format including a Console Report, Network Status Summary, Inventory Report, Identity and Access Summary, and Wireless Configuration Report. You can save these reports or send them to other users in the organization.

Related Information

- ExtremeAnalytics

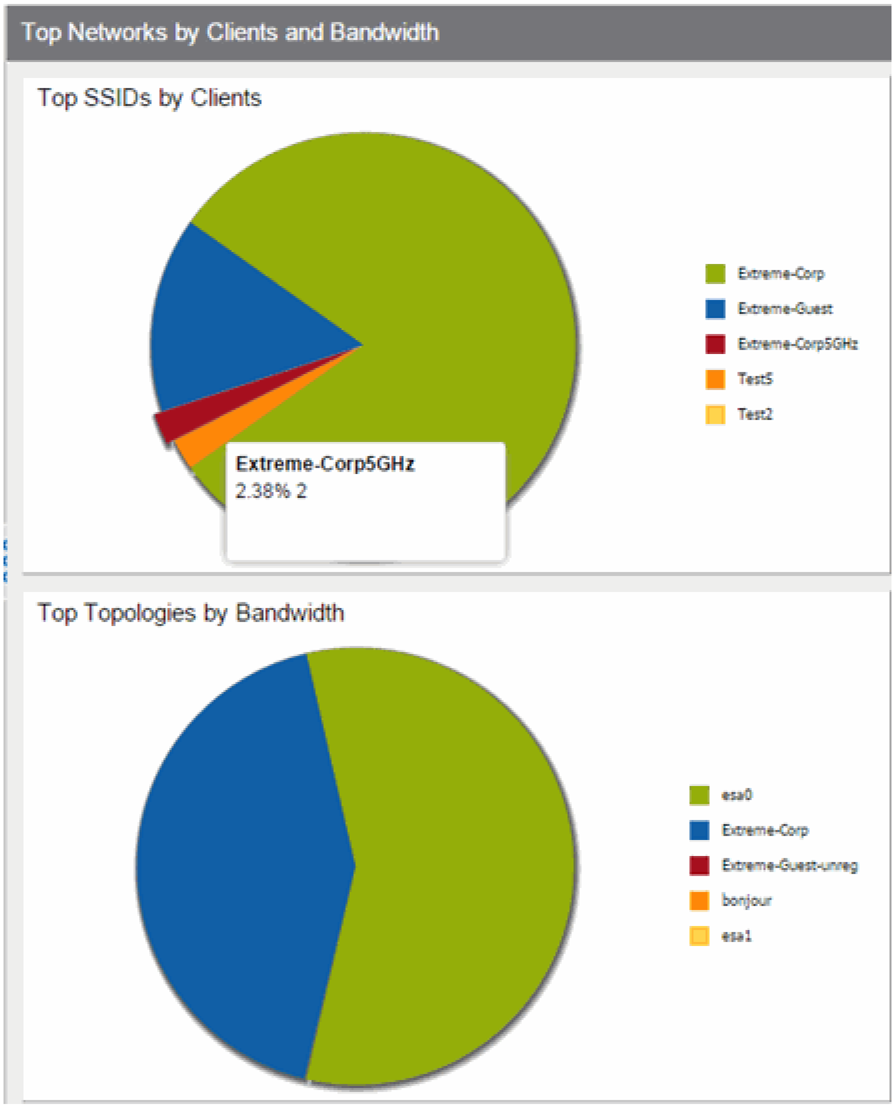
Reports Features

Extreme Management Center Reports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

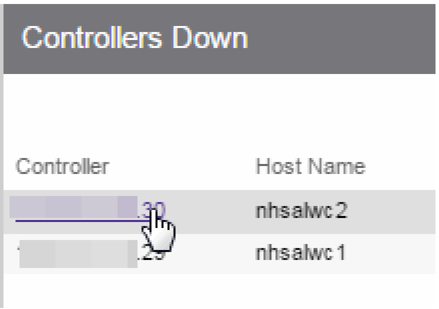
Reports Features

Extreme Management Center reports include the following features (depending on the report selected):

- Hover Over for Info — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, clicking on a pie section opens a filtered end-systems grid for more detailed information.



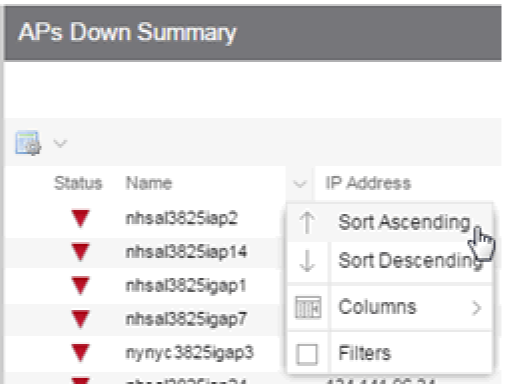
- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



Controllers Down

Controller	Host Name
[redacted]	nhsalwc2
[redacted]	nhsalwc1

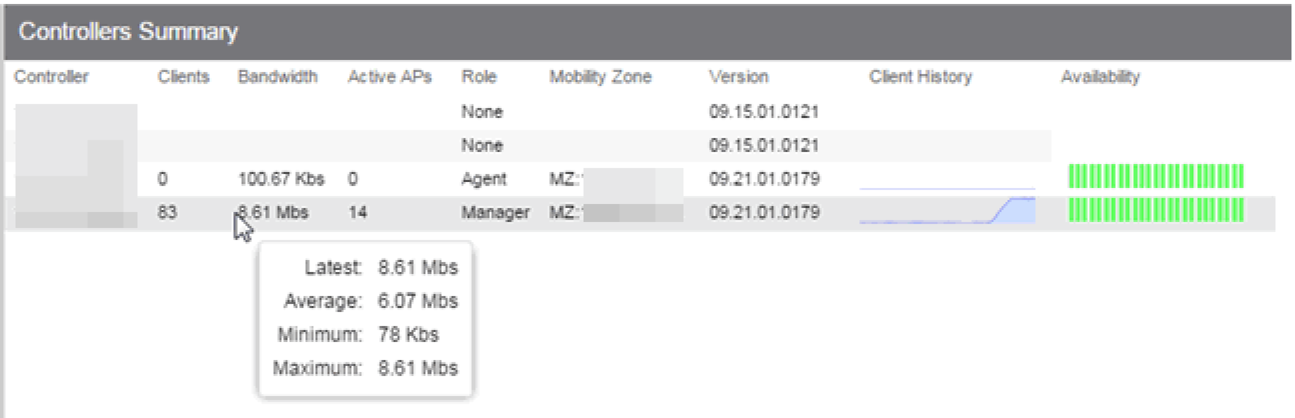
- Interactive Tables — Manipulate table data in several ways to customize the view for your own needs:
  - Click on the column headings to perform an ascending or descending sort on the column data.
  - Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
  - Filter, sort, and search the data in each column in the table.



APs Down Summary

Status	Name	IP Address
▼	nhsal3825iap2	
▼	nhsal3825iap14	
▼	nhsal3825igap1	
▼	nhsal3825igap7	
▼	nynyc3825igap3	

- 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.

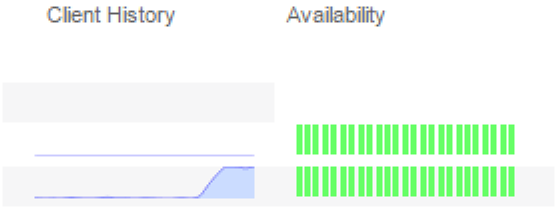


Controllers Summary

Controller	Clients	Bandwidth	Active APs	Role	Mobility Zone	Version	Client History	Availability
[redacted]				None		09.15.01.0121		
[redacted]				None		09.15.01.0121		
[redacted]	0	100.67 Kbs	0	Agent	MZ: [redacted]	09.21.01.0179		
[redacted]	83	8.61 Mbs	14	Manager	MZ: [redacted]	09.21.01.0179		

Latest: 8.61 Mbs
Average: 6.07 Mbs
Minimum: 78 Kbs
Maximum: 8.61 Mbs

- 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

- ExtremeAnalyticstab

Restoring an Extreme Management Center® Database Using the CLI

Use the instructions in this topic to restore a Extreme Management Center database backup using the CLI (command line). Restoring a database using the CLI may be necessary after making significant unwanted configuration changes.

NOTE: This topic assumes you previously created a database backup via the Backup/Restore tab.

The restore runs using the `mysqlbackup_restore` script in the `<install directory>\scripts` directory.

To restore the Extreme Management Center database backup:

1. Ensure you are running the **same version** of Extreme Management Center used when creating the database backup on the Extreme Management Center server.
2. Log into the system shell (via the local console or SSH) on the Extreme Management Center server as root on a Linux operating system or open a CMD prompt by selecting **Run as administrator** on a Windows operating system.
3. Navigate to the scripts directory:
   - On a Windows server, enter `cd "<install directory>"\scripts`.
   - On a Linux server, enter `cd <install directory>/scripts`.
4. Run the mysqlback_restore script:
   - On a Windows server, enter `mysqlbackup_restore.cmd "<full backup directory structure configured on Backup/Restore tab, including path>"`

     (e.g. `mysqlbackup_restore.cmd "C:\Program Files\Extreme Networks\NetSight\backup\netsight_03272017.sql"`).

   - On a Linux server, enter `./mysqlbackup_restore.sh <full backup directory structure configured on Backup/Restore tab, including path>`

     (e.g. `./mysqlbackup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/netsight_03272017.sql/`).

The database backup is restored.

Restore Device Configuration

On the **Network** tab, you can easily restore a device configuration to an active network device using a "cloned" configuration from an existing network device or a configuration template created on the **Network** > **Devices** tab. In addition, you also have the ability to download the latest firmware on the active device.

This Help topic provides the following information:

- Preliminary Steps
  - Required Capabilities
  - Device Firmware
- Restoring a Configuration
  - Using a Configuration Template
  - Cloning a Device Configuration

Preliminary Steps

Required Capabilities

In order to perform the restore configuration operation, you must be a member of an authorization group with the following capabilities.

Required Capability
Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard
Inventory Manager > Configuration Archive Management > Archive Restore Wizard
Inventory Manager > Configuration Templates Management > Configuration Templates Download Wizard
NetSight Suite > Devices > Add, Discover, and Import

Device Firmware

If you are updating the device's firmware, you must first add the new firmware version to the left-panel Firmware folder on the **Network** > **Firmware** tab. It is then available when configuring the device.

For information on obtaining firmware, contact your Extreme Networks representative, or access the firmware download library at: https://extremeportal.force.com/.

1. Place your new firmware in your firmware directory. Extreme Management Center uses the default tftpboot\firmware\images directory for storing your firmware.
2. In the left-panel Firmware folder, click the **Refresh** icon (🔄 Refresh). Extreme Management Center automatically adds your new firmware to the appropriate firmware groups in the left-panel Firmware folder.

The new firmware version is available when configuring the device in Extreme Management Center.

Restoring a Configuration

When restoring a configuration to an active device, there are two options for selecting a configuration to use. One option is to "clone" an existing device on the network for a configuration. Another option is to use a Configuration Template you create.

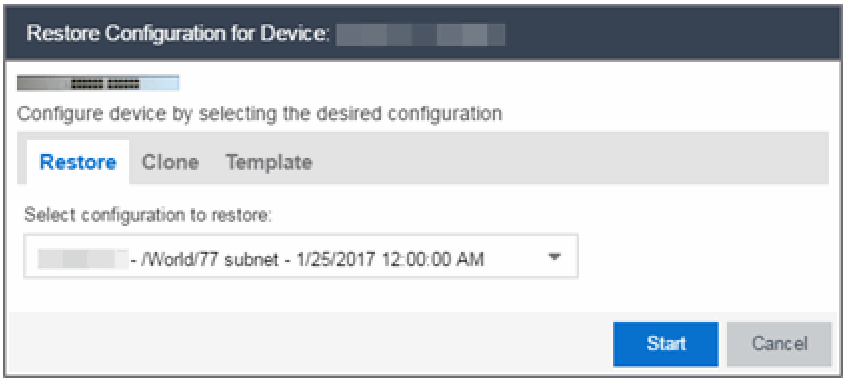
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived.

Using a configuration template allows you to restore a complete or partial configuration to the device with variables you can define specifically for that device. If you are going to use a configuration template for your device, you must create the Configuration Template to use as the source configuration for a device.

Cloning a Device Configuration

When cloning a device configuration, use an existing configuration of a network device archived in Inventory Manager. The cloned device (the archived device you are using) must **not** be active on the network to prevent two devices from having the same IP address on the network.

1. Launch Extreme Management Center. On the **Network** > **Devices** tab, right-click on the active device and select **Configuration/Firmware > Restore Configuration**. The Restore Configuration window opens.



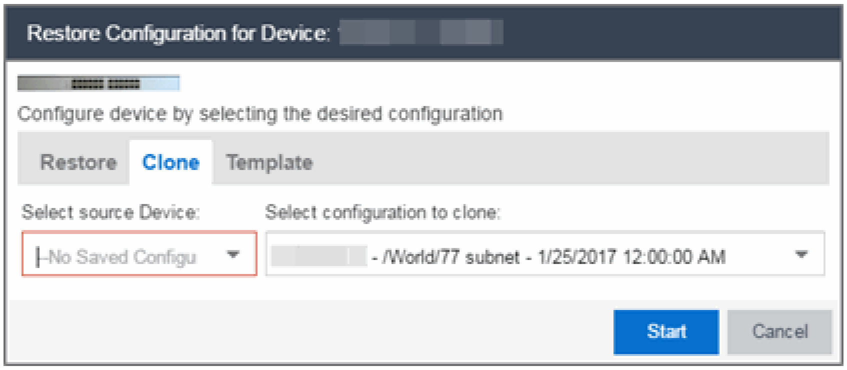
Restore Configuration for Device: [redacted]

Configure device by selecting the desired configuration

Select configuration to restore:

[redacted] - /World/77 subnet - 1/25/2017 12:00:00 AM

2. Select the **Clone** tab.



Restore Configuration for Device: [redacted]

Configure device by selecting the desired configuration

Select source Device: |-No Saved Configu

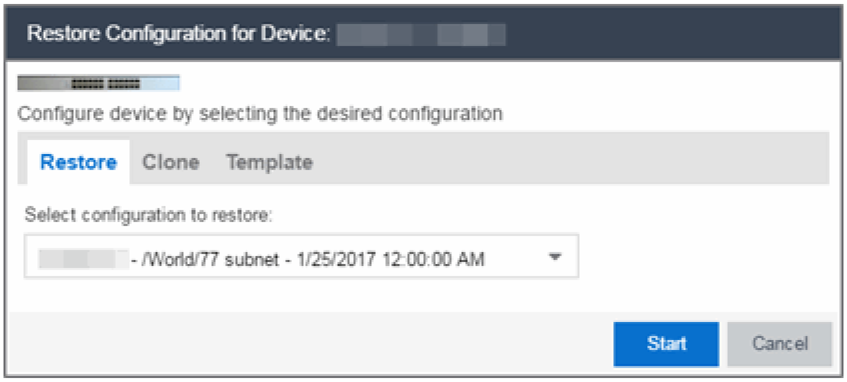
Select configuration to clone: [redacted] - /World/77 subnet - 1/25/2017 12:00:00 AM

3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to Inventory Manager. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. The selected device must be Inactive on the network or you cannot perform the restore operation. This prevents two devices from having the same IP address on the network.
6. Select the archived device configuration to clone.
7. Click **Start**. First, the firmware is updated (if that option is selected) and then the configuration is loaded and the device is restarted.

Using a Configuration Template

The following steps describe how to use a configuration template in Inventory Manager as the source configuration for a device.

1. Launch Extreme Management Center. On the **Network** > **Devices** tab, right-click on the active device and select **Configuration/Firmware > Restore Configuration**. The Restore Configuration window opens.



Restore Configuration for Device: [redacted]

[redacted]

Configure device by selecting the desired configuration

Select configuration to restore:

[redacted] - /World/77 subnet - 1/25/2017 12:00:00 AM

2. If desired, select a new version of firmware to download on the device. (You must add the new firmware version to Inventory Manager, see Device Firmware.)
3. Select the Template option as the Configuration Source.
4. Select the appropriate template from the **Template** drop-down menu and enter the required variables.
5. Select the Profile for the new device.
6. Click **Start**. First, the firmware is updated (if that option is selected), then, the configuration is loaded, the device is restarted, and the new IP address is added to Extreme Management Center.

Related Information

For information on related topics:

- Network Tab
- New Device Configuration in Extreme Management Center

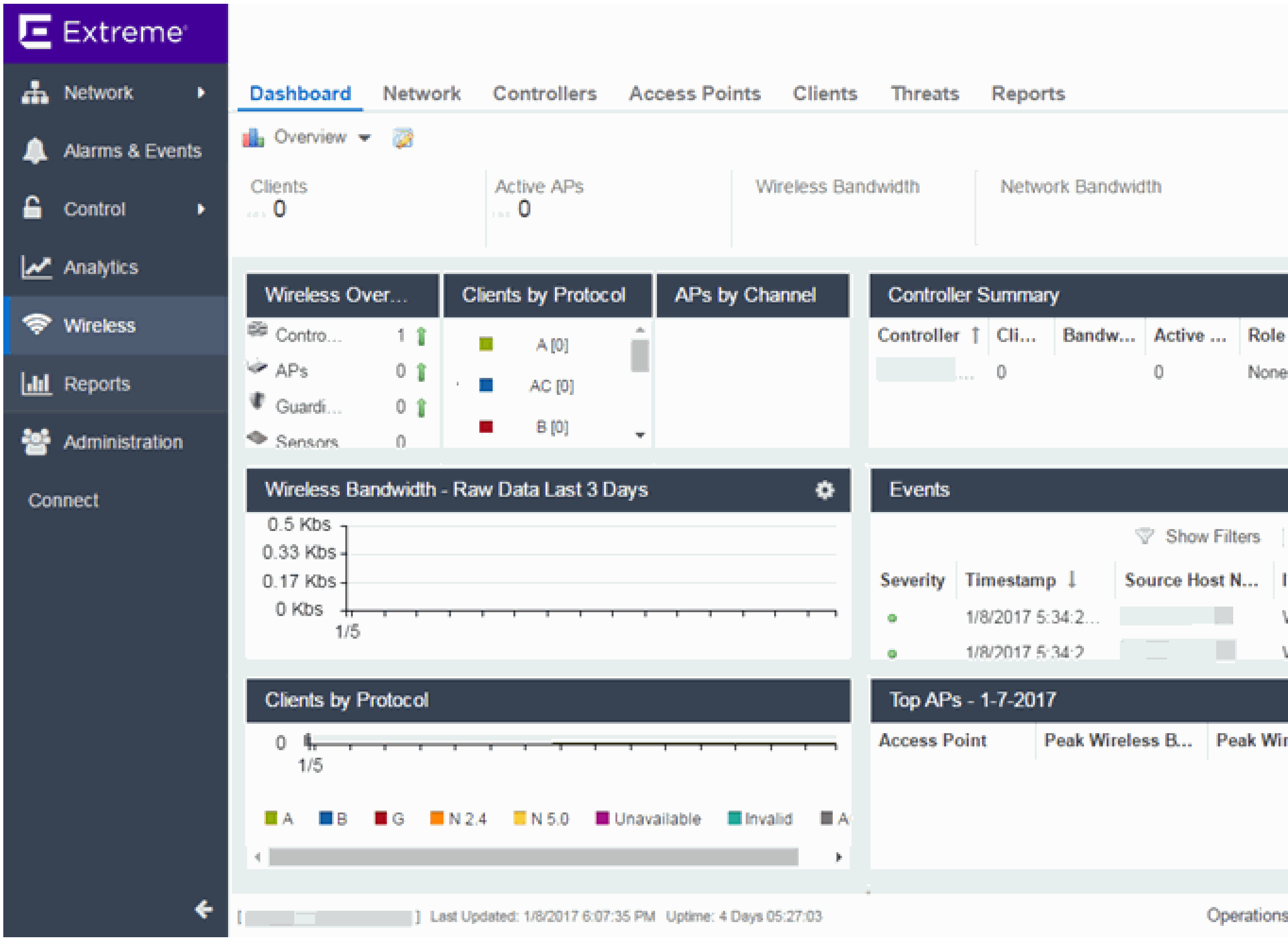
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21

When adding a Wireless Controller as a flow source in Extreme Management Center, a mirror port is automatically created. Wireless Controllers on which a firmware version of 10.21 or higher is installed use IPFIX, so the mirror port is unnecessary.

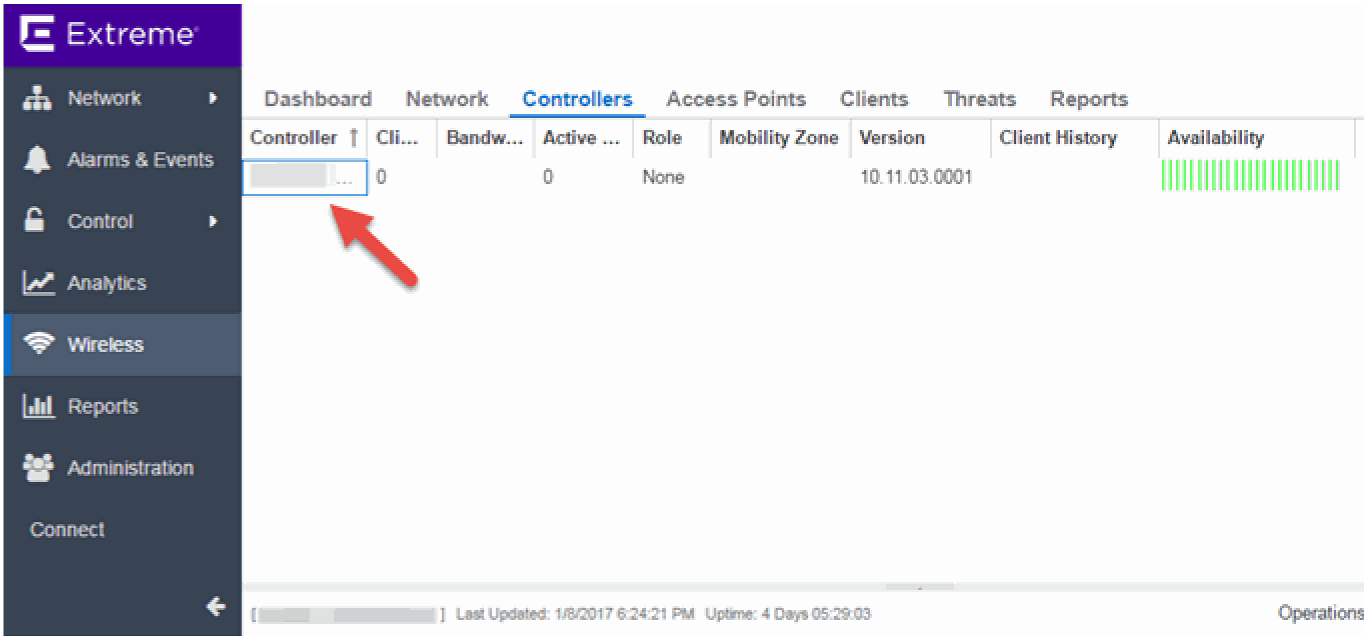
NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

To remove a mirror port on a Wireless Controller running version 10.21:

1. Access the **Wireless** tab in Extreme Management Center.
   The Wireless tab opens.



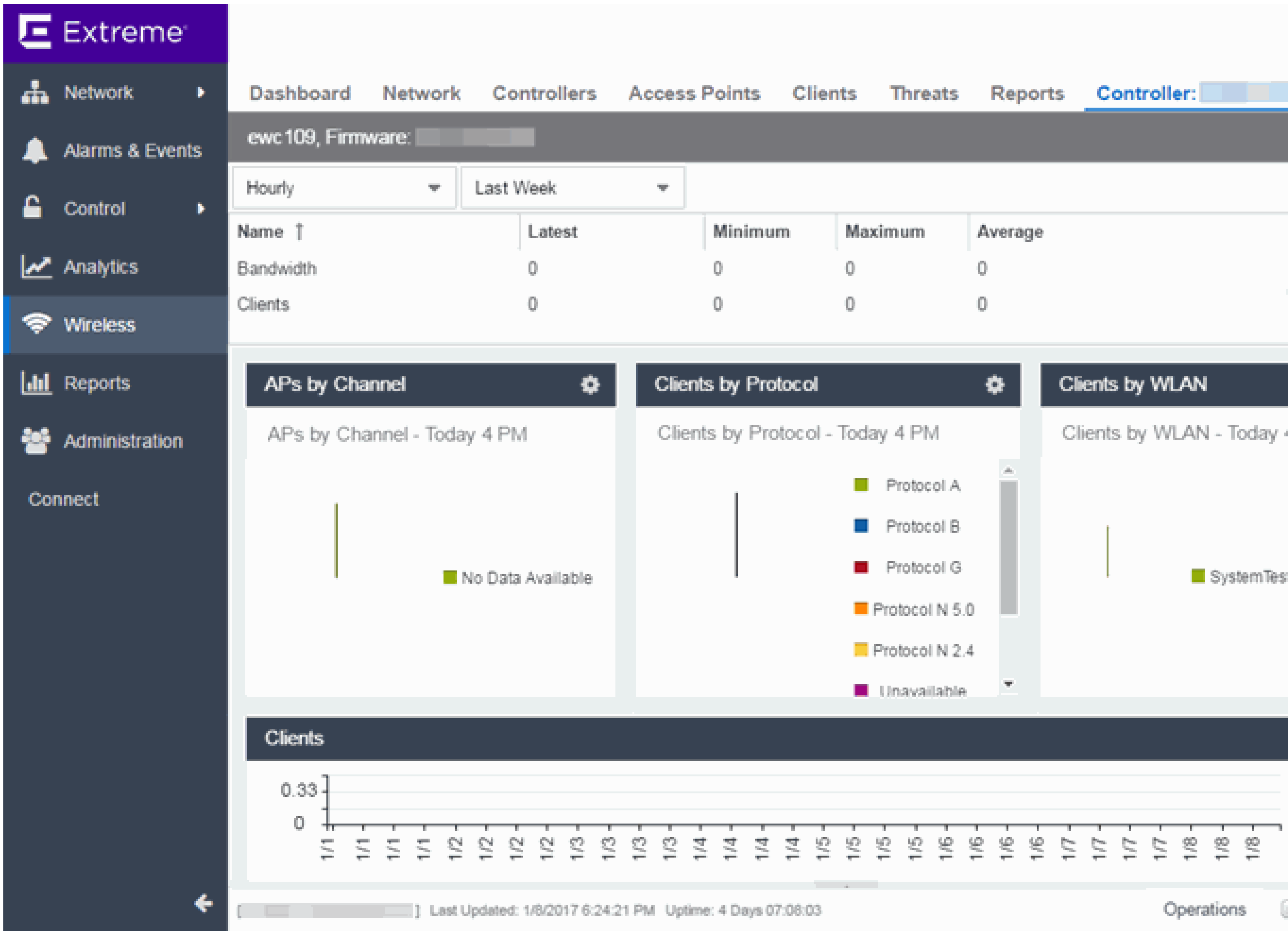
2. Select the **Controllers** tab.
   The Controllers tab opens.



Controller ↑	Cli...	Bandw...	Active ...	Role	Mobility Zone	Version	Client History	Availability
[redacted] ...	0		0	None		10.11.03.0001		

[[redacted]] Last Updated: 1/8/2017 6:24:21 PM Uptime: 4 Days 05:29:03

3. Click the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



ewc109, Firmware: [redacted]

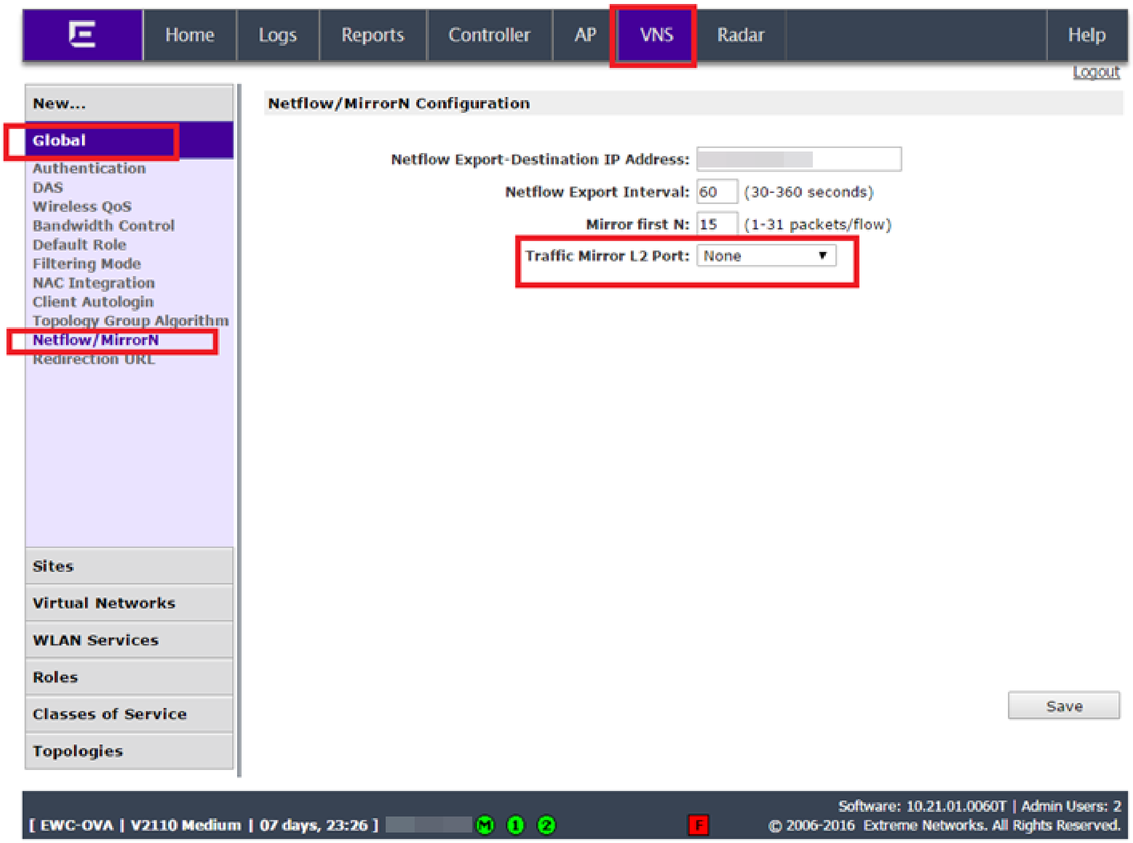
Hourly | Last Week

Name	Latest	Minimum	Maximum	Average
Bandwidth	0	0	0	0
Clients	0	0	0	0

[redacted] Last Updated: 1/8/2017 6:24:21 PM Uptime: 4 Days 07:08:03

4. Click the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.

5. Click the **VNS** tab.
   The **VNS** tab opens.



Netflow/MirrorN Configuration

Netflow Export-Destination IP Address: [redacted]
Netflow Export Interval: 60 (30-360 seconds)
Mirror first N: 15 (1-31 packets/flow)
Traffic Mirror L2 Port: None

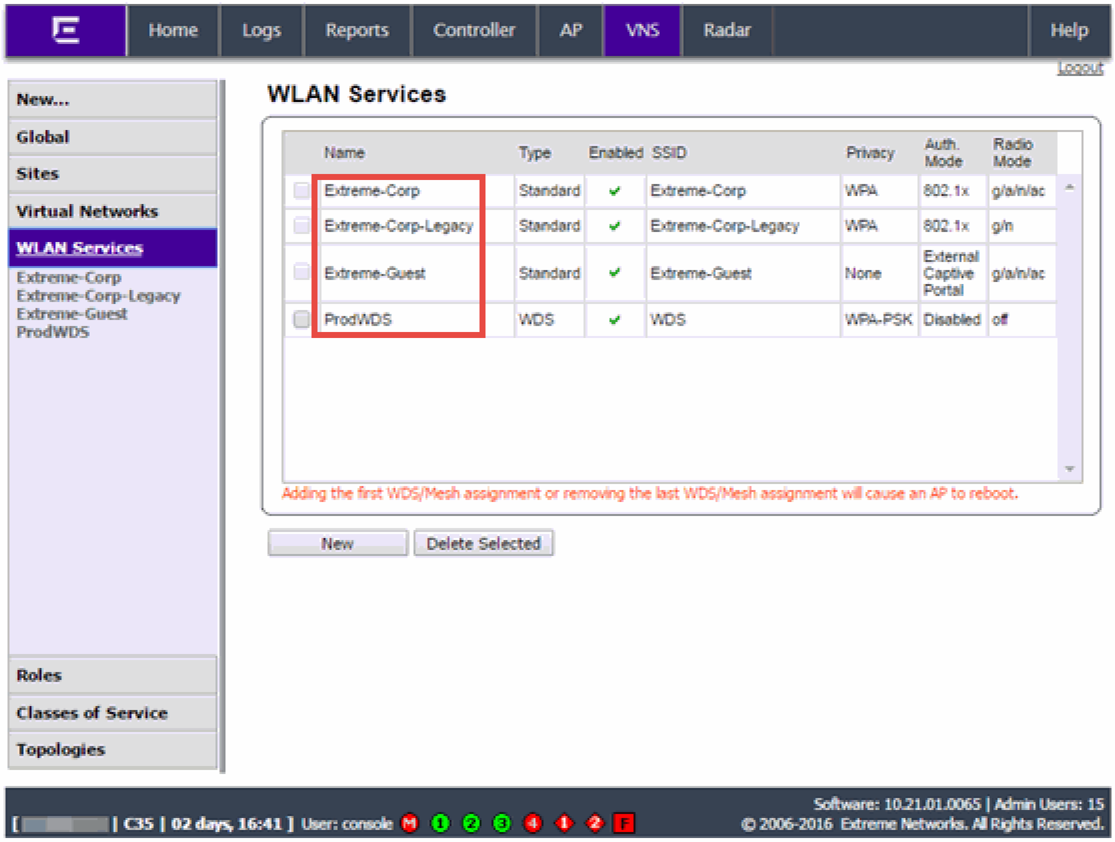
[EWC-OVA | V2110 Medium | 07 days, 23:26] [redacted]

Software: 10.21.01.0060T | Admin Users: 2
© 2006-2016 Extreme Networks. All Rights Reserved.

6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down menu.
8. Click the **Save** button.

NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > **Configuration** tab is not available once the **Traffic Mirror L2 Port** is disabled.

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.



WLAN Services

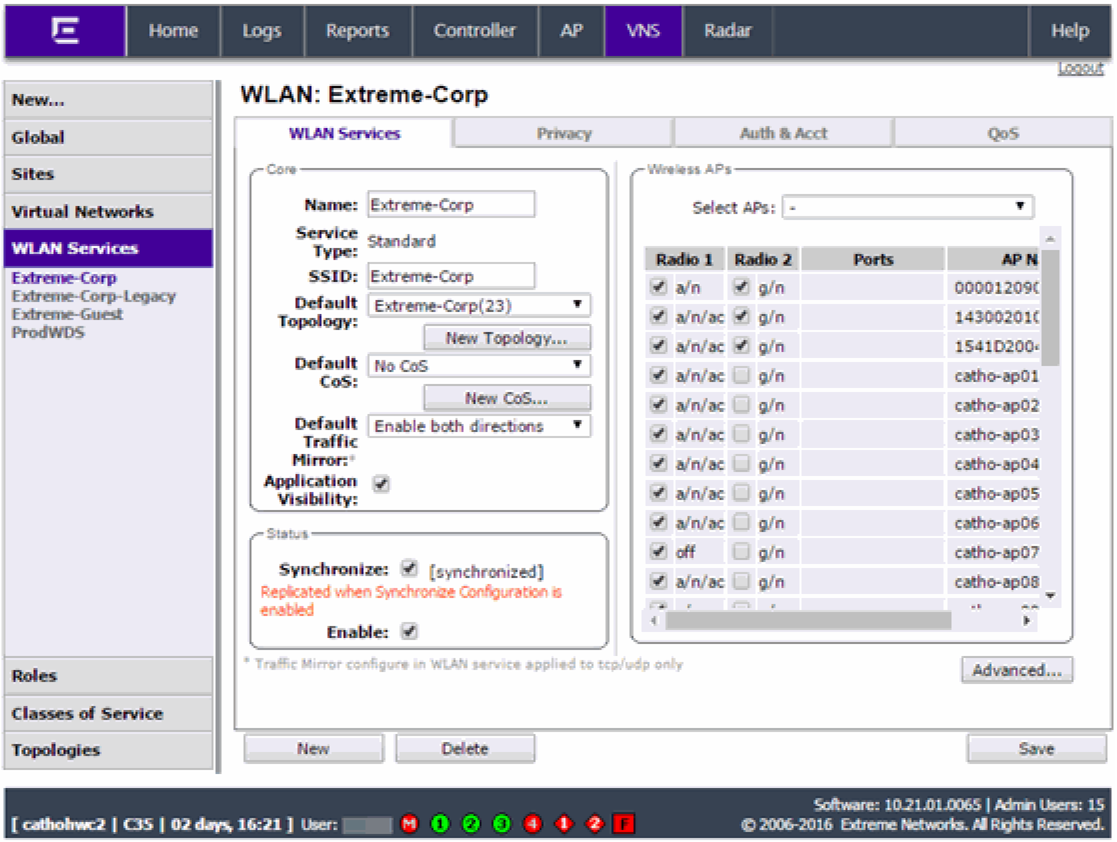
	Name	Type	Enabled	SSID	Privacy	Auth. Mode	Radio Mode
□	Extreme-Corp	Standard	✓	Extreme-Corp	WPA	802.1x	g/a/n/ac
□	Extreme-Corp-Legacy	Standard	✓	Extreme-Corp-Legacy	WPA	802.1x	g/n
□	Extreme-Guest	Standard	✓	Extreme-Guest	None	External Captive Portal	g/a/n/ac
□	ProdWDS	WDS	✓	WDS	WPA-PSK	Disabled	off

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

[[redacted] | C35 | 02 days, 16:41] User: console

Software: 10.21.01.0065 | Admin Users: 15
© 2006-2016 Extreme Networks. All Rights Reserved.

10. Click a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



WLAN: Extreme-Corp

Name: Extreme-Corp
Service Type: Standard
SSID: Extreme-Corp
Default Topology: Extreme-Corp(23)
Default CoS: No CoS
Default Traffic Mirror:* Enable both directions
Application Visibility: ☑

Synchronize: ☑ [synchronized]
Replicated when Synchronize Configuration is enabled
Enable: ☑

* Traffic Mirror configure in WLAN service applied to tcp/udp only

Select APs: -

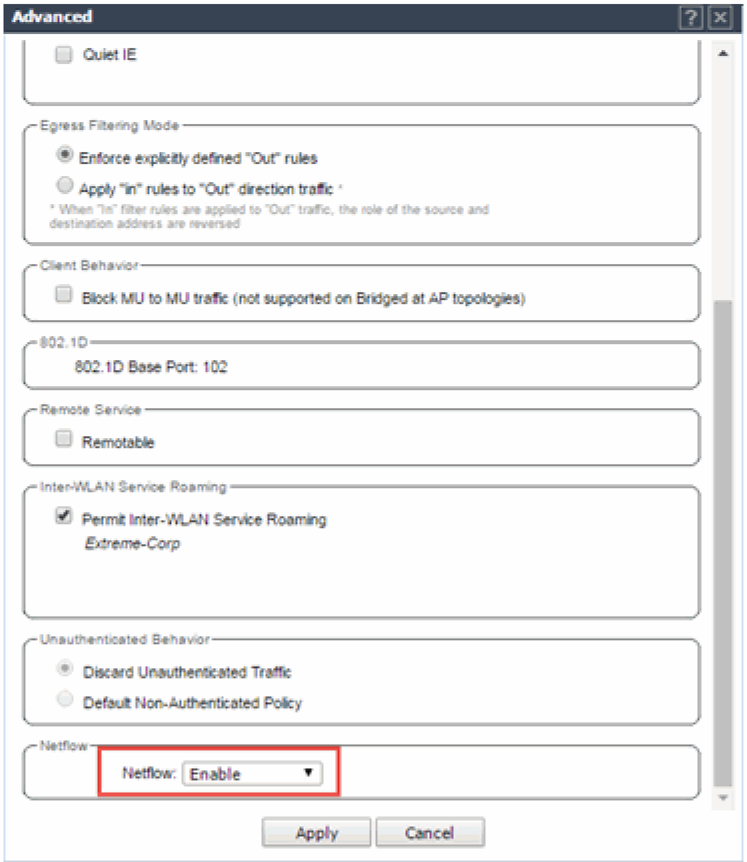
Radio 1		Radio 2		Ports	AP N
☑	a/n	☑	g/n		00001209(
☑	a/n/ac	☑	g/n		14300201(
☑	a/n/ac	☑	g/n		1541D200-
☑	a/n/ac	□	g/n		catho-ap01
☑	a/n/ac	□	g/n		catho-ap02
☑	a/n/ac	□	g/n		catho-ap03
☑	a/n/ac	□	g/n		catho-ap04
☑	a/n/ac	□	g/n		catho-ap05
☑	a/n/ac	□	g/n		catho-ap06
☑	off	□	g/n		catho-ap07
☑	a/n/ac	□	g/n		catho-ap08

[cathohwc2 | C35 | 02 days, 16:21] User: [redacted] M 1 2 3 4 1 2 F

Software: 10.21.01.0065 | Admin Users: 15
© 2006-2016 Extreme Networks. All Rights Reserved.

11. Click the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down menu is set to **Enable**.



Advanced

□ Quiet IE

Egress Filtering Mode

● Enforce explicitly defined "Out" rules

○ Apply "in" rules to "Out" direction traffic *

* When "In" filter rules are applied to "Out" traffic, the role of the source and destination address are reversed

Client Behavior

□ Block MU to MU traffic (not supported on Bridged at AP topologies)

802.1D

802.1D Base Port: 102

Remote Service

□ Remotable

Inter-WLAN Service Roaming

☑ Permit Inter-WLAN Service Roaming

Extreme-Corp

Unauthenticated Behavior

● Discard Unauthenticated Traffic

○ Default Non-Authenticated Policy

Netflow

Netflow: Enable

13. Click the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** may incorrectly be **0** when flow data is gathered via a wireless controller running version 10.21 or higher. Additionally, application response times and some meta data may be blank. This is a known issue and will be addressed in a future release.

Related Information

For information on related topics:

- Wireless

How to Configure ExtremeXOS Identity Manager to Send Events to Extreme Management Center

This chapter describes how to use the Identity Management — Configuration script on a Summit series or Black Diamond series switch to send events to Extreme Management Center.

In order to run the Identity Management — Configuration script on a device, you must be a member of an authorization group assigned the Extreme Management Center Suite > Common Web Services > Web Services APIs Read/Write Access capability.

To run the Identity Management — Configuration script on a device:

1. Open the **Network** > **Devices** tab in Extreme Management Center.
2. Right-click a Summit series or Black Diamond series switch in the Devices table or in the Device Groups left-hand panel.
3. Select the Identity Management — Configuration script in the Scripts > Extreme Access Control menu. The Run Script window opens.
4. On the **Device Selection** tab, the selected device is automatically included. Use the arrows to add additional devices or remove devices and to control the order of the selected devices.
5. Click **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. If desired, click the **Description** tab to view the description defined for the script.
    - Stop on error? — Indicates whether the script stops if an error occurs.
    - Target Server IP Address — The IP address to which notifications are sent.
        - Entering a value of $serverIP automatically enters the IP address of the Extreme Management Center server IP.
        - Enter the IP address of the Extreme Access Control engine if using the Extreme Networks ExtremeControl solution.
    - Target Server Type — Selecting netsight monitors the IP, username, and port of the user accessing the device. Users with the Extreme

Networks ExtremeControl solution can select nac, which provides you with the ability to run Kerberos authentication (if enabled) on the device.

NOTE: In order to give elevated access to users when using the Kerberos authentication type on the device, the Target Server Type must be **nac** to allow the Access Control engine to learn the Kerberos traffic.

- Target Server Username — The username of the user to which the web service request is made.
- Target Server Password — The password of the user to which the web service request is made.
- Target Server HTTPs Port — The port that the Extreme Management Center server or Access Control engine uses for HTTPS communication. The default port is 8443, but if the port was changed when configuring the Extreme Management Center server or Access Control engine, enter the custom port used.
- XML Target Name — The name of the targets on the switch to which IDM events are sent. Using the default predefined XML Target Name creates a unique name for each server.
- Choose Action — The action that occurs on the device when the script is run.
  - Enable ID Monitoring — This option sets up the XML notification, configures ports for Identity Management (if specified), and enables or disables ports for devices you can use with Identity Management.
  - Manage Ports — This option only configures ports for Identity Management (if specified).

7. On the Run-Time Settings tab, set the run-time settings for the script (for more information about defining run-time variables when creating a script, see Specifying Run-Time Settings for a Script).
   - Save configuration in the background after running script successfully — Device configuration is saved after the script is run.
   - Timeout if script is not completed on each device (in seconds) — The amount of time in seconds before a timeout occurs if a device does not respond.
   - Run now, don’t save as a task — Select to run the script now and do not save the script as a task.

- Save as a task and run now — Select to run the script now and save it as a task. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Creating Script Tasks").
- Save as task. I'll run later — Select to save running the script as a task. The script does not run at this time. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Creating Script Tasks").

8. Click **Next**. On the Verify Run Script tab, verify your script selections, and then click **Next**.
9. Click **Next**.
10. On the Results tab, you see the results of the script including any errors.
11. Click **Close**.

How to Create Scripts

This chapter describes the scripting functionality built into Extreme Management Center, and how to use Extreme Management Center to create scripts.

Extreme Management Center Script Overview

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Extreme Management Center scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

Extreme Management Center allows you to create Extreme Management Center tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

Extreme Management Center scripts are similar to ExtremeXOS scripts in that they are collections of ExtremeXOS CLI commands and control structures. Extreme Management Center scripts add some additional commands specific to Extreme Management Center.

In general, Extreme Management Center scripts support syntax and constructs from the following sources:

- ExtremeXOS CLI commands — ExtremeXOS CLI commands in a Extreme Management Center script are sent to the device or port and the response can be used by the script. Abbreviated ExtremeXOS commands do not work unless you prefix the shortened command with CLI. For example, to abbreviate show vlan, type `CLI sh vlan`.
- ExtremeXOS CLI scripts — Control structures such as IF..ELSE and DO..WHILE can be used in Extreme Management Center scripts. See "CLI Scripting" in the *ExtremeXOS User Guide* for more information on ExtremeXOS script functionality and syntax.
- 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 Extreme Management Center scripts, see "Tcl Support in Extreme Management Center Scripts".

  Syntax and constructs from these sources work seamlessly within Extreme Management Center scripts. For example, the response from a switch to an ExtremeXOS CLI command issued from a script can be processed using Tcl functions.

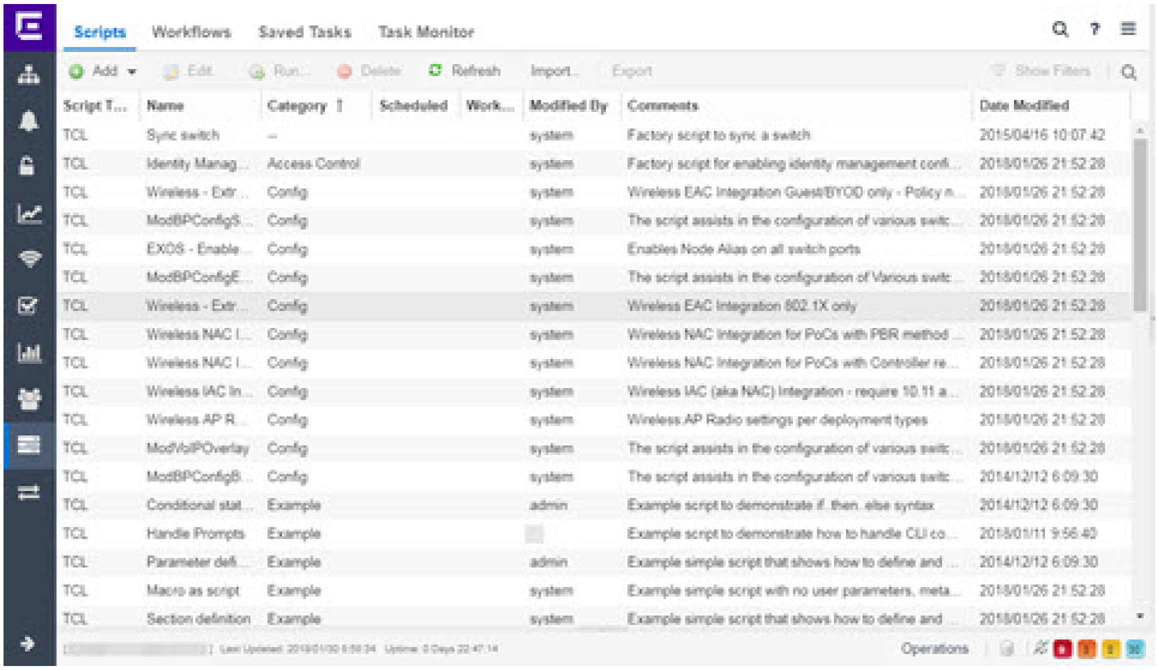
Bundled Extreme Management Center Scripts

Extreme Management Center includes a number of sample scripts you can use as templates for your own Extreme Management Center scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with Extreme Management Center are available to users with an Administrator role. The XML source files for the scripts are located at `<`*`install directory`*`>\appdata\scripting\bundled_scripts`.

The Extreme Management Center Script Interface

To display the scripts configured in Extreme Management Center, select the **Tasks** tab, then click the **Scripts** subtab.



Script T...	Name	Category	Scheduled	Work...	Modified By	Comments	Date Modified
TCL	Sync switch	--			system	Factory script to sync a switch	2015/04/16 10:07:42
TCL	Identity Manag...	Access Control			system	Factory script for enabling identity management confi...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration Guest/BYOD only - Policy n...	2018/01/26 21:52:28
TCL	ModBPConfigS...	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	EXOS - Enable...	Config			system	Enables Node Alias on all switch ports	2018/01/26 21:52:28
TCL	ModBPConfigE...	Config			system	The script assists in the configuration of Various switc...	2018/01/26 21:52:28
TCL	Wireless - Extr...	Config			system	Wireless EAC Integration 802.1X only	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with PBR method...	2018/01/26 21:52:28
TCL	Wireless NAC I...	Config			system	Wireless NAC Integration for PoCs with Controller re...	2018/01/26 21:52:28
TCL	Wireless IAC In...	Config			system	Wireless IAC (aka NAC) Integration - require 10.11 a...	2018/01/26 21:52:28
TCL	Wireless AP R...	Config			system	Wireless AP Radio settings per deployment types	2018/01/26 21:52:28
TCL	ModVoIPOverlay	Config			system	The script assists in the configuration of various switc...	2018/01/26 21:52:28
TCL	ModBPConfigB...	Config			system	The script assists in the configuration of various switc...	2014/12/12 6:09:30
TCL	Conditional stat...	Example			admin	Example script to demonstrate if..then..else syntax	2014/12/12 6:09:30
TCL	Handle Prompts	Example				Example script to demonstrate how to handle CLI co...	2018/01/11 9:56:40
TCL	Parameter defi...	Example			admin	Example simple script that shows how to define and ...	2014/12/12 6:09:30
TCL	Macro as script	Example			system	Example simple script with no user parameters, meta...	2018/01/26 21:52:28
TCL	Section definition	Example			system	Example simple script that shows how to define and ...	2018/01/26 21:52:28

Last Updated: 2019/01/30 8:58:34 Uptime: 0 Days 22:47:14

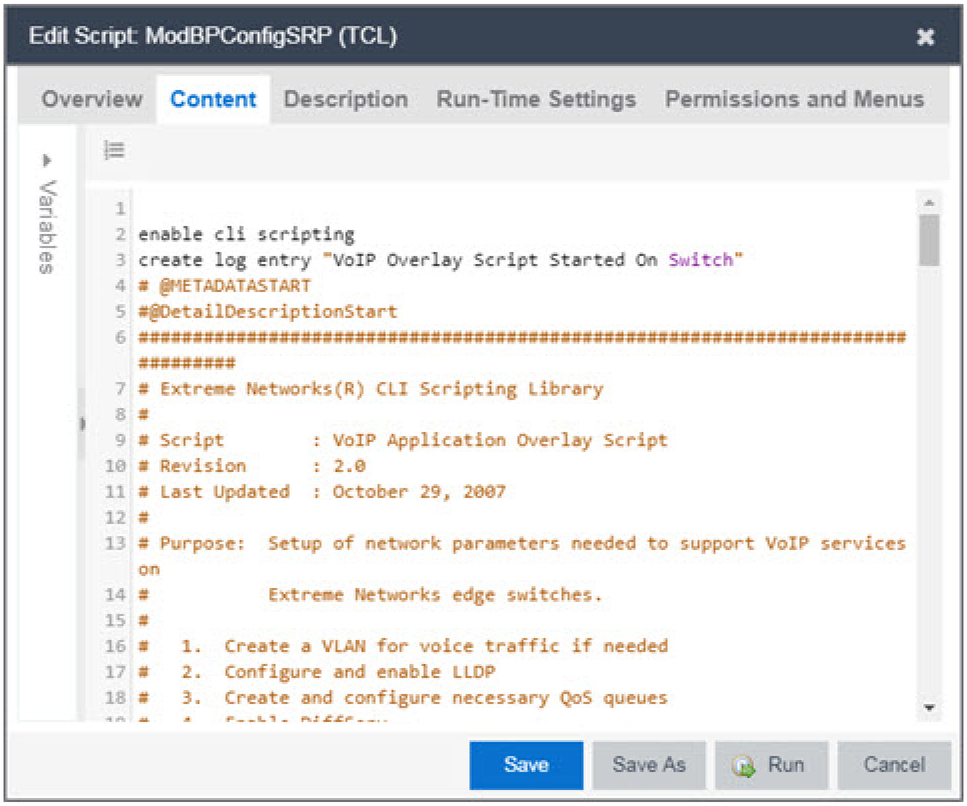
The **Scripts** tab contains the following information:

- **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** — The name of the last user to modify the script.
- **Date Modified** — The date the script was last modified.

The **Saved 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 saved task.
- **User Name** — The name of the last user to modify the saved task.
- **Script Name** — The name of the script run by the script task.
- **Comment** — Comments or a description of the script task.
- **Date Modified** — The date the script task was last modified.

Double-click a script to open the script editor dialog.



```

enable cli scripting
create log entry "VoIP Overlay Script Started On Switch"
# @METADATASTART
#@DetailDescriptionStart
##########################################################################################
# Extreme Networks(R) CLI Scripting Library
#
# Script        : VoIP Application Overlay Script
# Revision      : 2.0
# Last Updated  : October 29, 2007
#
# Purpose:  Setup of network parameters needed to support VoIP services on
#           Extreme Networks edge switches.
#
#    1.  Create a VLAN for voice traffic if needed
#    2.  Configure and enable LLDP
#    3.  Create and configure necessary QoS queues
```

The Extreme Management Center script editor allows you to add content to a script, set values for parameters, specify run-time settings, and indicate the Extreme Management Center users that can run the script.

The following tabs appear in the Extreme Management Center **Script Editor** window:

- **Overview** — Displays fields to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
- **Content** — Displays the script in a text editor window, where you can modify it directly.
- **Description** — Contains descriptive information about the script. The script description is specified in the metadata section of the script.
- **Run-Time Settings** — Specifies script settings applied when the script is run.
- **Permissions and Menus** — Specifies Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.

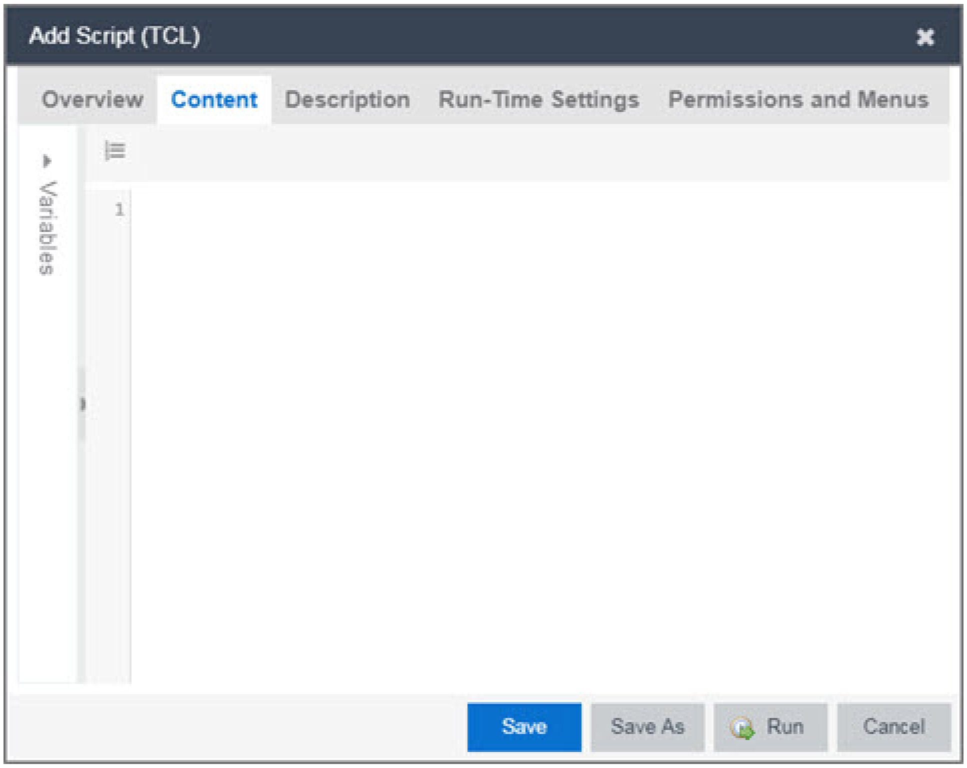
Managing Extreme Management Center Scripts

With scripting, you can:

- Create an Extreme Management Center Script
- Specify Run-Time Settings for a Script
- Specify Permissions and Run Locations for Scripts
- Run a Script
- View Script Results
- Edit a Script
- Delete a Script
- Import Scripts into Extreme Management Center
- Export a Script
- Configure Script Tasks

Create an Extreme Management Center Script

1. On the **Tasks** tab, click **Scripts**.
2. Click the **Add** button and select the type of script you are creating:
3. Select the type of script you are creating:
   - **TCL** — Tool Command Language
   - **Python** — Python script
   - **JSON-RPC-CLI** — Machine to Machine Interface (used to send CLI commands to an ExtremeXOS device).
   - **JSON-RPC-Python** — Machine to Machine Interface (used to send a Python script to an ExtremeXOS device).
4. The Add Script dialog box appears.



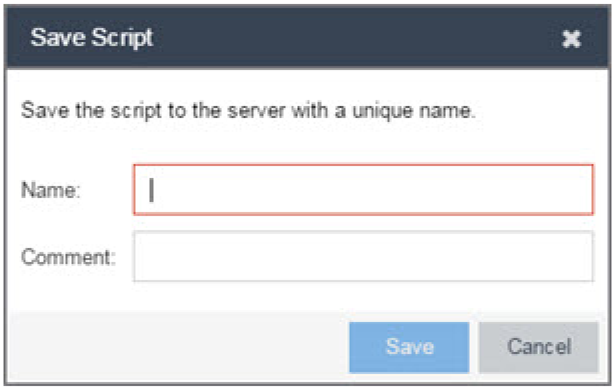
5. Type the metadata tags `#@DetailDescriptionStart` and `#@DetailDescriptionEnd` between the tags `#@MetaDataStart` and `#@MetaDataEnd`, and then type a detailed description between these detailed description tags. This description appears on the **Description** tab.
6. Place variable definition statements in the metadata section (between `#@MetaDataStart` and `#@MetaDataEnd` tags).

   Variables can be defined by expanding the Variables menu on the left of the **Content** tab. A list of system variables appears under Variables. To add a variable to the script, double-click the variable.
7. Enter the script commands after the metadata section of the script. For information about what can appear in a Extreme Management Center script, see Extreme Management Center Script Reference.

   The following are examples of valid script commands:

   - ExtremeXOS 12.1 and later CLI scripting commands
   - TCL commands
   - Constructs

8. Click the **Run-Time Settings** tab and make changes as need if you want to specify run-time settings. For additional information, see Specifying Run-Time Settings for a Script.
9. To specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu, click the **Permissions And Menus** tab and make changes as needed. For additional information, see Specifying Permissions and Run Locations for Scripts.
10. Click **Save**. The Save Script dialog box appears.



Save Script

Save the script to the server with a unique name.

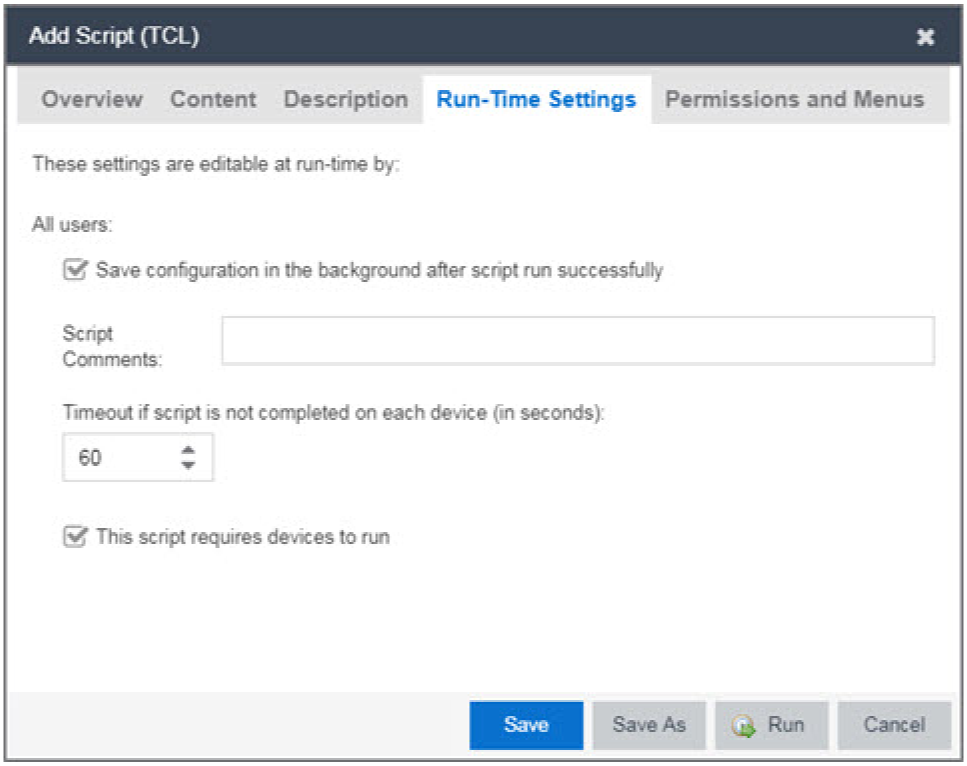
Name:

Comment:

11. 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.
12. Click **Save**.
13. Click **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Run-Time Settings for a Script

To specify the run-time settings for a script, click the **Run-Time Settings** tab.



Add Script (TCL)

These settings are editable at run-time by:

All users:

☑ Save configuration in the background after script run successfully

Script Comments:

Timeout if script is not completed on each device (in seconds):

60

☑ This script requires devices to run

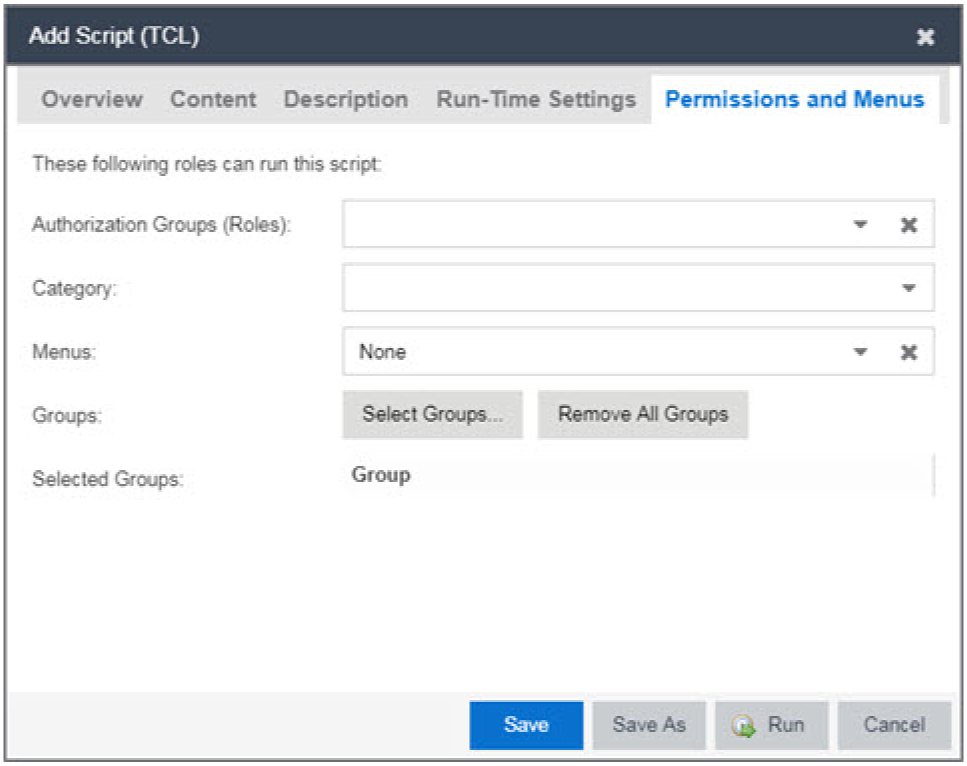
Use this tab to specify the following settings:

- **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 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 or port (in seconds). This timeout value applies to each device or port independently.

Specify Permissions and Run Locations for Scripts

Specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.

Click the **Permissions and Menus** tab to set permissions and menu locations for the script.


Add Script (TCL)

These following roles can run this script:

Authorization Groups (Roles):

Category:

Menus: None

Groups:

Selected Groups: Group

- Specify the Extreme Management Center user roles able to see and run the script. Select the check boxes for the roles you wish to enable.
- Set if and where the script appears in the menu and in a shortcut menu in the given locations.

Run 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 devices and to control the order of the selected devices.
4. Click **Next**.
5. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, click the **Description** tab to view the description defined for the script.
6. Click **Next**.

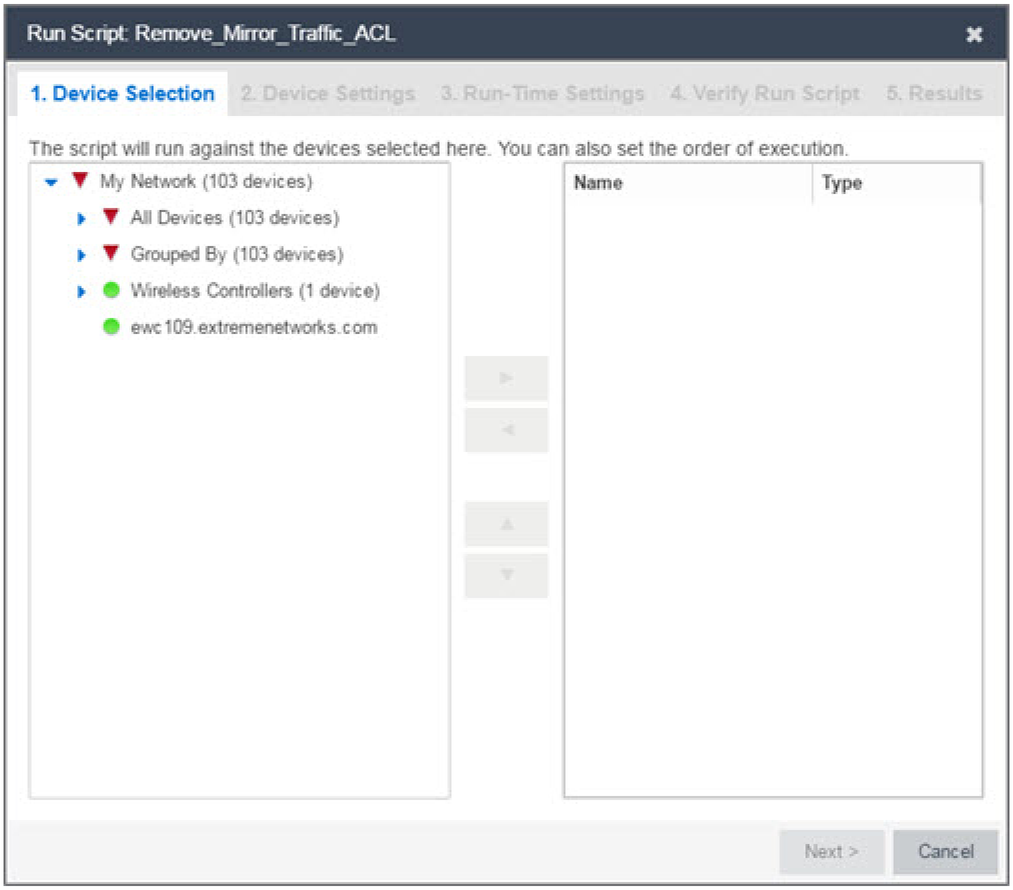
7. On the **Run-Time Settings** tab, set the run-time settings for the script. For additional information, see Specifying Run-Time Settings for a Script.
    - **Save configuration in the background after script run successfully** — When selected, the configuration on the device is saved after the script 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 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 Create Script Tasks.
    - **Save as a 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 Create 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 Tasks tab:

1. Click **Scripts**.
2. On the **Scripts** tab, find the script in the list. If needed, filter the list by typing search terms in the search box.
3. Select the script by clicking its row and then click **Run**. The Run Script window opens.

NOTE: Be sure to select only one script. The **Run** button is unavailable if two or more scripts are selected.

4. On the **Device Selection** tab, shown below, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the selected devices.


Run Script: Remove_Mirror_Traffic_ACL
1. Device Selection
2. Device Settings
3. Run-Time Settings
4. Verify Run Script
5. Results
The script will run against the devices selected here. You can also set the order of execution.
My Network (103 devices)
All Devices (103 devices)
Grouped By (103 devices)
Wireless Controllers (1 device)
ewc109.extremenetworks.com
Name
Type
Next >
Cancel

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 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 Create Script Tasks.
- **Save as a 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 Create 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**.

View Script Results

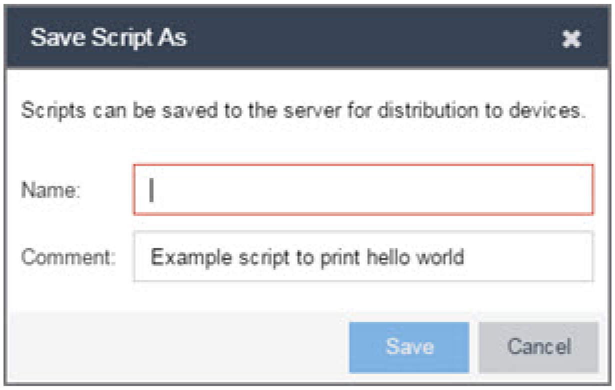
Once a script is run, results are stored in the `<install directory>/appdata/scripting/tmp` folder. The folder in which script results are stored cannot be configured.

An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. Once the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select the script you want to edit.
3. Click the **Edit** button. The script opens in the Edit Script window, where you can edit the script.
4. Click **Save As**. The **Save Script As** dialog box appears.



Scripts can be saved to the server for distribution to devices.

Name:

Comment: Example script to print hello world

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.

Delete a Script

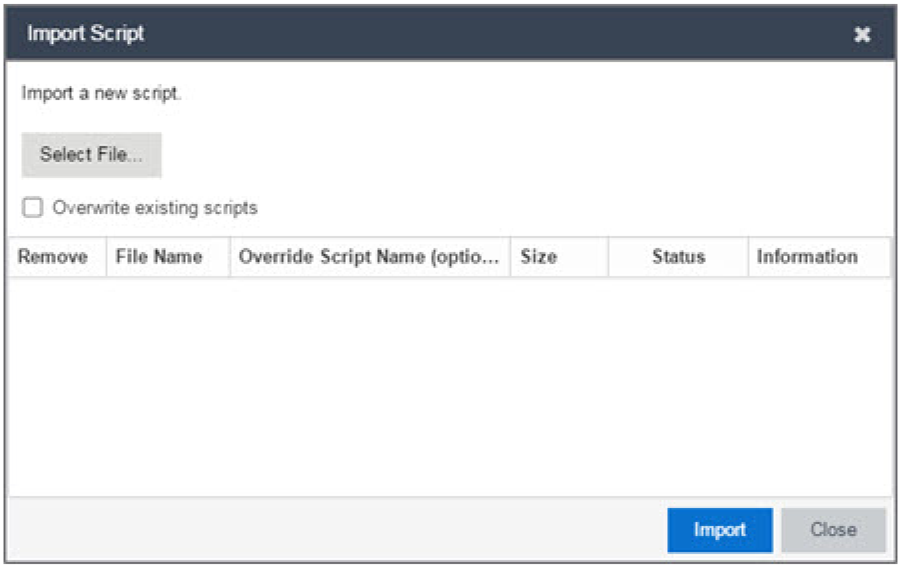
To delete a script:

1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the script deletion.

Import Scripts into Extreme Management Center

Import XML-formatted scripts into Extreme Management Center. To import a script:

1. In the **Tasks** tab, click **Scripts**.
2. Click the **Import** button.


Import Script

Import a new script.

□ Overwrite existing scripts

Remove	File Name	Override Script Name (optio...	Size	Status	Information

3. Click **Select File** to navigate to the location of the script. The script appears in the grid.
4. Enter a new Script Name in the Override Script Name (optional) field if you want to edit the name of the script.
5. Click **Import**.
6. Verify the script is imported and click **Close**.

NOTE: Exported EPICenter 6.0 telnet macros cannot be imported as XML scripts.

Export a Script

To export a script:

1. From the **Tasks** tab, select a script.
2. Click the **Export** button.

The script is exported in XML format to your browser download directory.

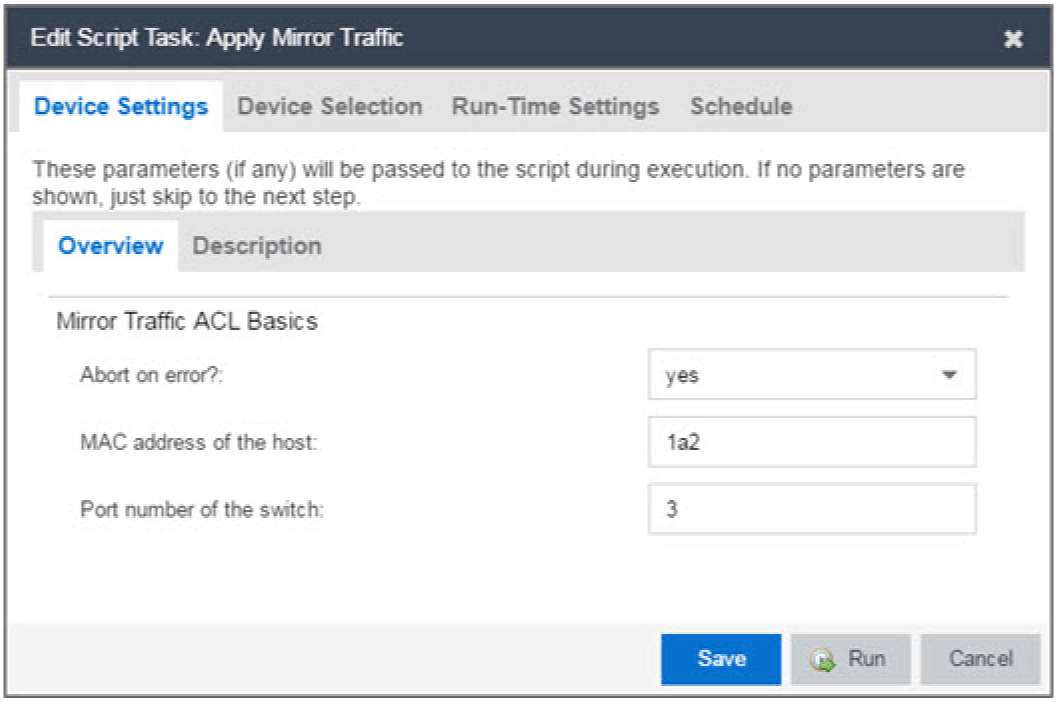
Configure Script Tasks

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 a regular basis.

Create Saved Tasks

To create a saved task, you need to:

1. Select a script or workflow.
2. Run the script or workflow and designate it as a task by selecting either **Save as a task and run now** or **Save as task. I'll run later** on the **Run-Time Settings** tab.
3. Click the **Saved Tasks** tab.
4. Double-click the saved task or click the saved task and click **Open**. The Edit Saved Task window appears (see the following figure).



Edit Script Task: Apply Mirror Traffic

These parameters (if any) will be passed to the script during execution. If no parameters are shown, just skip to the next step.

Mirror Traffic ACL Basics

Abort on error?: yes

MAC address of the host: 1a2

Port number of the switch: 3

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 on the **Schedule** tab to schedule the script task to run automatically.
   a. Click the **Schedule Task** button.
   b. Select the script task you want to run in the **Saved Task Name** drop-down menu.

c. Enter a **Task Name** and **Description** for the scheduled task in the Task Details section.

d. Select how often you want the scheduled task to run in the Recurrence Pattern section.

e. Select the starting and ending date and time to run the script task using the **Start** and **End** date and time fields in the Date/Time Range section of the window.

f. Enter the scheduled task recipient's email address in the **To** field and enter any information you want to include in the email when the scheduled task is sent in the **Subject** and **Body** fields.

g. Click **Save**.

   The saved task is now scheduled to run automatically on the date and time you configured.

8. Click **Save** to save any changes.
9. Click **Run** to run the saved task or **Cancel** to exit the script task.

Deleting Saved Tasks

If desired, delete saved tasks you no longer need. To delete a saved task:

1. Remove any schedules configured (Scheduled = Recurring or One-time) with the saved task by clicking the **Saved Tasks** tab, selecting the associated schedule, and clicking **Delete**.
2. Select the **Tasks** tab, click the **Saved Tasks** tab.
3. Select the saved task in the table.
4. Click the **Delete** button.

Extreme Management Center Script Reference

This section contains reference information for Extreme Management Center scripts. It contains the following topics:

- Metadata Tags
- Extreme Management Center-Specific Scripting Constructs
- Tcl Support in Extreme Management Center Scripts
- Entering Special Characters

- Line Continuation Character
- Case Sensitivity in Extreme Management Center Scripts
- Reserved Words in Extreme Management Center Scripts
- ExtremeXOS CLI Scripting Commands Supported in Extreme Management Center Scripts
- Extreme Management Center-Specific System Variables

A Extreme Management Center script may contain a metadata section, which can serve as a usability aid in the script interface. The metadata section, if present, is the first section of a Extreme Management Center script, followed by the script logic section, which contains the CLI commands and control structures in the script. The metadata section is delimited between `#@MetaDataStart` and `#@MetaDataEnd` tags. A metadata section is optional in a Extreme Management Center script.

Use metadata tags to specify the description of the script, as well as parameters that the script user can input. The information specified by the metadata tags appears in the **Overview** tab for the script.

Metadata Tags

#@MetaDataStart and #@MetaDataEnd

Indicates the beginning and end of the metadata section of the script. In order for description information and variable input fields to appear in the **Overview** tab for a script, the corresponding metadata tags must appear in the metadata section.

Example

```
#@MetaDataStart

#@SectionStart (description = "Protocol Configuration
Section") Set var protocolSelection eaps

#@SectionEnd

#@SectionStart (description = "vlan tag section") Set var
vlanTag 100

#@MetaDataEnd
```

#@ScriptDescription

Specifies a one-line description of the script. The description specified with this tag cannot contain a newline character.

Example

```
#@ScriptDescription "This is a VLAN configuration script."
```

#@DetailDescriptionStart and #@DetailDescriptionEnd

Specifies the beginning and end of the detailed description of the script. The detailed description can be multiple lines or multiple paragraphs. The detailed description is shown in the **Script View** tab in the script editor window.

Example

```
#@DetailDescriptionStart

#This script performs configuration upload from Extreme
Management Center to the switch.

#The script only supports tftp.

#This script does not support third party devices.

#@DetailDescriptionEnd
```

#@SectionStart and #@SectionEnd

Specifies the beginning and end of a section within the metadata part of a script. 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 Extreme Management Center:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response

- Synchronizing the Device with Extreme Management Center
- Saving the Configuration on the Device Automatically
- Printing a String to the Output File

Specifying the Wait Time Between Commands

After the script executes a command, the sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
sleep 5
```

Example

```
# sleep for 5 seconds after executing a command

sleep 5
```

Printing System Variables

The printSystemVariables command prints the current values of the system variables. Specifically, values for the following variables are printed:

- deviceIP
- deviceName
- serverName
- deviceSoftwareVer
- serverIP
- serverPort
- date
- time
- abort_on_error
- CLI.OUT

Syntax

```
printSystemVariables
```

Example

```
# Display values for system variables
```

```
printSystemVariables
```

Configuring a Carriage Return Prompt Response

A special string within the script, `<cr>`, indicates a carriage return in response to a prompt for a command.

Syntax

```
<cr>
```

Example

```
# cancel download
```

```
download image 10.22.22.22 t.txt <cr>
```

Synchronizing the Device with Extreme Management Center

The PerformSync command manually initiates a synchronization for specified Extreme Management Center feature areas and scope.

Syntax

```
PerformSync [-device <ALL | deviceIp>] [-scope <EAPSDomain |
VPLS> ]
```

If -device is not specified, the current device (indicated by the `$deviceIP` system variable) is assumed.

The PerformSync command is executed in an asynchronous manner so when the command is executed, Extreme Management Center moves on to the next command in the script without waiting for the PerformSync command to complete.

Examples

```
PerformSync -scope VPLS
```

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 Extreme Management Center scripts:

after	concat	for	info	lrange	puts	set	unset
append	continue	foreach	interp	lreplace	read	split	update
array	eof	format	join	lsearch	regexp	string	uplevel
binary	error	gets	lappend	lsort	regsub	subst	upvar
break	eval	global	lindex	namespace	rename	switch	variable
catch	expr	history	linsert	open	return	tell	vwait
clock	fblocked	if	list	package	scan	time	while
close	flush	incr	llength	proc	seek	trace	

See www.tcl.tk/man/tcl8.2.3/TclCmd/contents.htm for syntax descriptions and usage information for these Tcl commands.

Entering Special Characters

In a Extreme 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 Extreme Management Center script.

Line Continuation Character

The line continuation character is not supported in Extreme Management Center scripts. Place each command statement on a single line.

Case Sensitivity in Extreme Management Center Scripts

The commands and constructs in a Extreme Management Center script are not case-sensitive. However, if a command is referenced inside another command, the inner command is case-sensitive. In this instance, the inner command case matches how it appears in the Extreme Management Center documentation.

Example (Usage of the Extreme Management Center command ECHO)

```
echo hi (valid)

echo [echo hi] (error)

echo [ECHO hi] (valid)
```

Reserved Words in Extreme Management Center Scripts

The following words cannot be used as variable names in a Extreme Management Center script. They are reserved by Extreme Management Center.

- Names of system variables (see Extreme Management Center-Specific System Variables)
- Names of Extreme Management Center command extensions (see Extreme Management Center-Specific Scripting Constructs)
- Names of ExtremeXOS CLI commands
- Names of Tcl functions

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

Extreme Management Center scripts support the CLI commands in this section.

- `$VAREXISTS`
- `$TCL`
- `$UPPERCASE`
- `show var`
- `delete var`
- `configure cli mode scripting abort-on-error`

$VAREXISTS

- Checks if a given variable is initialized.
- Switch Compatibility — Devices running ExtremeXOS 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given Tcl command. The following constructs support the $TCL command:
- `set var if`
  - while
- See Tcl Support in Extreme Management Center Scripts for a list of supported Tcl commands.
- Switch Compatibility — Devices running ExtremeXOS 11.6 and higher support this command.
- Example — `set var foo $TCL(expr 3+4) if ($TCL(expr 2+2) == 4) then`

$UPPERCASE

- Converts a given string to upper case.
- The following constructs support the $UPPERCASE command:
  - set var
  - if
  - while
- Switch Compatibility — Devices running ExtremeXOS 11.6 and higher support this command.

NOTE: The $UPPERCASE command is deprecated in ExtremeXOS 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $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 Extreme Management Center scripts:

$abort_on_error

Whether the script terminates if a CLI error occurs; 1 aborts on error, 0 continues on error.

$CLI.OUT

The output of the last CLI command.

$CLI.SESSION_TYPE

The type of session for the connection to the device, either Telnet or SSH.

NOTE: Variables with TCL special characters must be enclosed in braces. For example, when using the system variables `$CLI.SESSION_TYPE` and `$CLI.OUT` in a script, they must be entered as `${CLI.SESSION_TYPE}` and `${CLI_OUT}`, respectively.

$date

The current date on the Extreme Management Center server.

$deviceIP

The IP address of the selected device.

$deviceLogin

The name of the login user for the selected device.

$deviceName

The DNS name of the selected device.

$deviceSoftwareVer

The version of ExtremeXOS running on the selected device.

$deviceType

The product type of the selected device.

$netsightUser

The name of the Extreme Management Center user running the script.

$isExos

Indicates whether the device is an ExtremeXOS device. Possible values are True or False.

$port

Selected port numbers, represented as a string. If the script is not associated with a port, this system variable is not supported.

$serverIP

The IP address of the Extreme Management Center server.

$serverName

The host name of the Extreme Management Center server.

$serverPort

The port number used by the Extreme Management Center web server; for example, 8080.

$STATUS

The execution status of the previously executed ExtremeXOS command: 0 if the command executed successfully, non-zero otherwise.

$time

The current time on the Extreme Management Center server.

$vendor

Vendor name of the device; for example, Extreme.

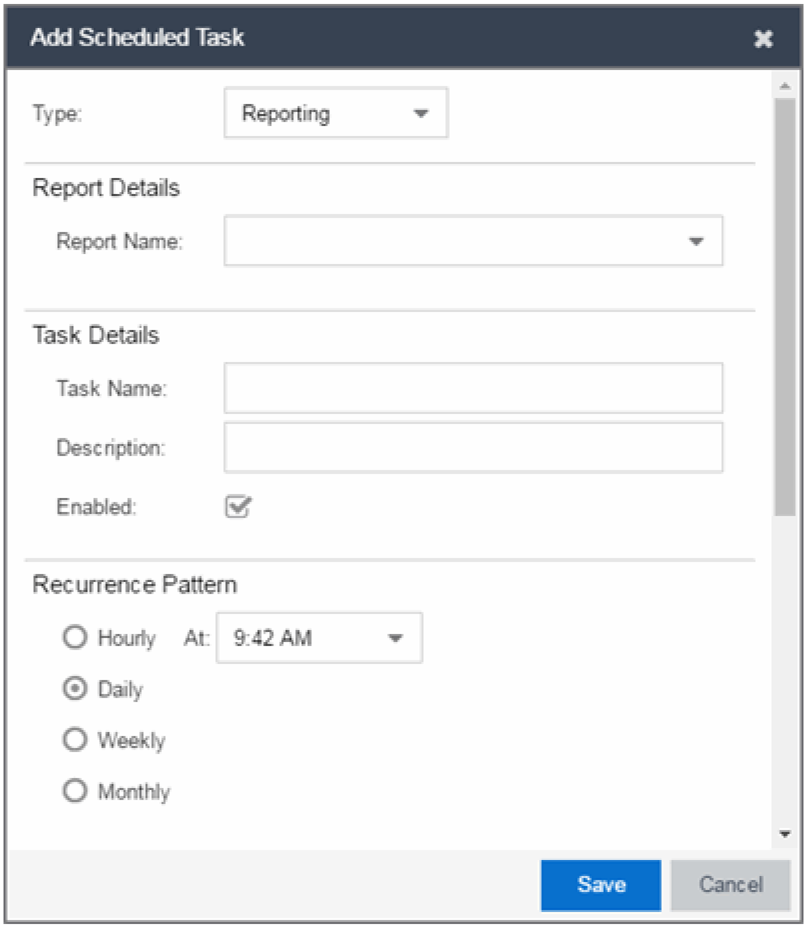
How to Schedule a Task

The **Scheduled Task** tab allows you to configure Extreme Management Center to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a script or workflow
- Email information to Extreme Networks Support
- Discover newly added devices

To create a new task:

1. Launch Extreme Management Center.
2. Select the **Tasks** tab and select the **Scheduled Tasks** tab.
3. Click the **Add** button. The Add Scheduled Task window opens.



Add Scheduled Task

Type: Reporting

Report Details

Report Name:

Task Details

Task Name:

Description:

Enabled: ☑

Recurrence Pattern

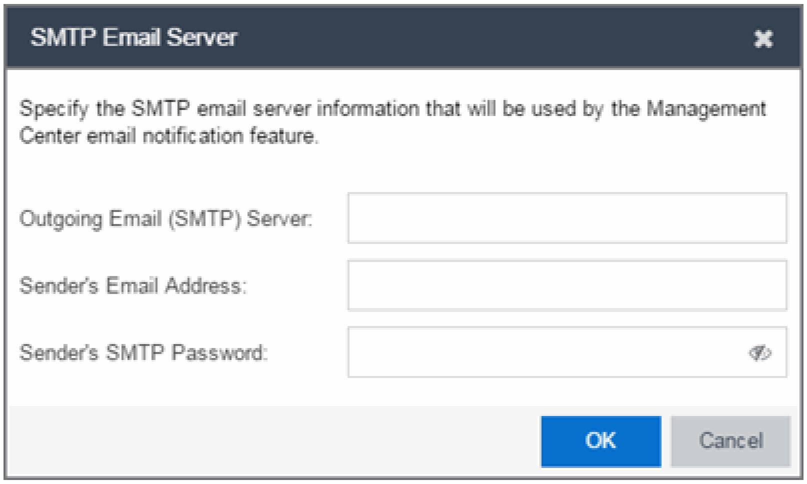
○ Hourly At: 9:42 AM

● Daily

○ Weekly

○ Monthly

If no SMTP email settings are configured, the SMTP Email Server window also opens, where you can define the SMTP email settings. You can also configure the SMTP email settings in the SMTP Email Options tab.



SMTP Email Server

Specify the SMTP email server information that will be used by the Management Center email notification feature.

Outgoing Email (SMTP) Server:

Sender's Email Address:

Sender's SMTP Password:

4. Enter the outgoing SMTP email settings, if necessary, and click **OK**.
5. Select the type of task from the **Type** drop-down menu in the Add Scheduled Task window:
    - **Reporting** — Emails a report you select (created on the Report Designer tab) on a scheduled basis.
    - **Saved Task** — Runs a task saved on the Saved Tasks tab and sends an email on a scheduled basis.
    - **Support** — Emails debugging data on a scheduled basis that provides information to Extreme Networks Support in the event of an issue with your network. ***Only select this option if instructed to do so by Extreme Networks Support.***
    - **Site** — Runs a device discover for a site (created on the Site tab) on a scheduled basis.
    - **Disable Alarms** — Disables enabled alarms for the amount of time you define on a scheduled basis. Use this task to avoid alarms during times you reserve for network maintenance activity. You can manually ignore enabled alarms on the Alarm Configuration tab.
6. Select the report, saved task, support task, or site you want to schedule in the **Report Name**, **Saved Task Name**, **Support Task Name**, or **Site to Discover** drop-down menu, respectively. Depending on what you select, you may need to make other selections such as specifying the source engine or controller.
7. Edit the task name and description, if desired.
8. Select or deselect the **Enabled** checkbox to enable or disable the task, respectively. A disabled task is not performed.
9. Select whether you want the task to occur on an hourly, daily, weekly, or monthly basis.
    - **Hourly** — specify the minute each hour you want the task performed.
    - **Daily** — specify the time each day you want the task performed.
    - **Weekly** — specify the day or days of the week and the time you want the task performed.
    - **Monthly** — specify the day of the month and the time you want the task performed.
10. Specify a start and end date and time for the task, if desired.

11. Enter the email address or list of email addresses (separated by semicolons) where you want the generated PDF reports sent.
12. Enter the subject line and body text for the email, if desired.
13. Click **Save**. The task appears in the Scheduled Tasks table.

    Additionally, use the toolbar buttons to edit, copy, or delete the task. The **Refresh** button updates the Scheduled Tasks table to display any recent changes. Clicking the **Disable** button causes a task not to run without deleting it from the Scheduled Tasks table.

    Click the **Run** button to run the scheduled task immediately, if desired.

    Click the **SMTP** button to open the SMTP Email Server window to edit your outgoing email options.

Related Information

For information on related topics:

- Tasks
- SMTP Email Options

FlexViews

FlexViews provide a convenient way for Operations people to view device data. These views are accessible from Extreme Management Center Devices and do not require the installation of any software (including Extreme Management Center) other than the browser itself.

To launch a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

This Help topic provides information on the following topics:

- Browser Requirements
- Launching FlexViews
- Using FlexViews
    - Setting the Auto Refresh Interval
    - Editing Writable Values

Browser Requirements

The following web browsers are supported:

- Microsoft Edge and Internet Explorer version 11
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

Enable JavaScript in your browser for the views to function. To avoid impaired functionality, enable cookies for your browser. This includes (but is not limited to) the ability to persist table configurations such as filters, sorting, and column selections.

Launching FlexViews

Use the following steps to launch and open a FlexView from the **Network** tab. The maximum number of FlexViews you can open at one time is 10.

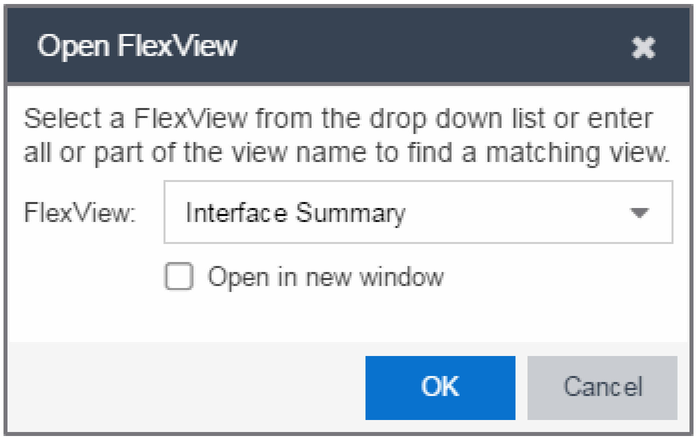
1. Launch Extreme Management Center and click on **Network** > **Devices**.
2. Select one or more devices in the Devices list.

   NOTE: When you select multiple devices, a FlexView may take additional time to populate with data, depending on the number of rows displayed in the particular view. Because of this, we recommend that, for interface-based FlexViews, you select five devices or fewer.

3. Click the **Menu** icon (☰) and select **View** > **FlexView** from the menu. You can also double-click the device in the Devices table to launch a FlexView.

   The Open FlexView window opens.

4. Select a FlexView from the drop-down menu, or enter all or part of the FlexView name to find a matching view. Any FlexView configured is listed for selection, including standard FlexViews and custom FlexViews you create.

   Select a FlexView from the drop down list or enter all or part of the view name to find a matching view.

   FlexView: Interface Summary

   ☐ Open in new window

   The FlexView opens in a new browser tab.

Using FlexViews

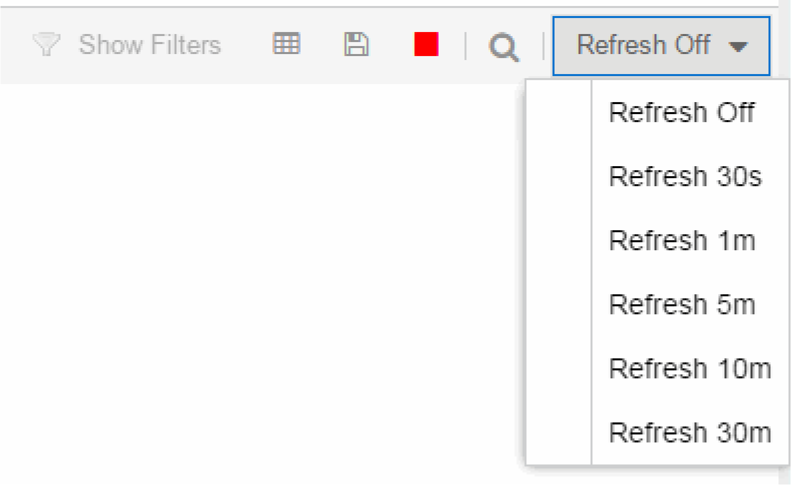
FlexViews let you manipulate the table data in several ways to customize the view for your own needs:

- Click on the column headings to sort column data in ascending or descending order.
- Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
- Rearrange columns by dragging a column heading to the desired position.
- Use the **Search** field to filter on and search for specific FlexView data.
- Set a Refresh Interval, which automatically refreshes the data at the specified interval.
- Edit the values in FlexView table columns containing a writable MIB object.

NOTE: Row creation and data exports are not currently supported in FlexViews.

Setting the Refresh Interval

Use the Refresh drop-down menu to specify an interval (in seconds) at which the FlexView data is automatically refreshed. To stop auto refresh, select the **Refresh Off** option.

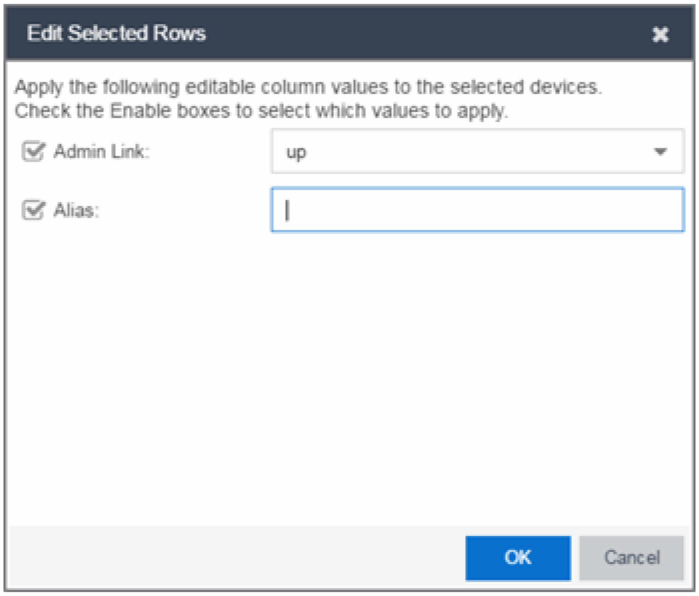


Editing Writable Values

You can change the value in FlexView table columns that contain a writable MIB object.

1. Select one or more rows in the FlexView that contain columns with writable MIB objects, right-click and select **Edit Selected Rows**.

   The Edit Selected Rows window opens.



Edit Selected Rows

Apply the following editable column values to the selected devices.
Check the Enable boxes to select which values to apply.

☑ Admin Link: up

☑ Alias:

2. Select the writeable objects you are changing and enter the appropriate values as needed.

   NOTE: Adding an alias to a port configures both Extreme Management Center and the CLI of the switch to display the character string.

3. Click OK to enter your changes into the selected rows. The new values are written directly to the device.

Related Information

For information on related topics:

- Network

Troubleshooting

This troubleshooting guide provides a list of items to check when Extreme Management Center functionality is failing to perform correctly. Locate a problem in the left column and then review the troubleshooting information in the right column.

Problem	Troubleshooting Steps
Error contacting a wireless controller. The controller shows a Warning icon. ⚠.	1. Verify that the Configuration password in the CLI Credential used for this device is properly configured. a. From Extreme Management Center, access **Administration** > **Profiles** tab. b. Select the **CLI Credentials** subtab. c. Select the CLI Credential being used by the controller's Profile, and click **Edit**. d. Verify the user name and password used in the credential. For wireless controllers, add the Login password to the Configuration password field instead of the Login password field. The username and Configuration password specified here must match the username and Login password configured on the controller. e. Verify the SSH connection type is selected. f. Click **OK**. g. Use this CLI Credential in the controller's Profile. **NOTE:** When configuring profiles for ExtremeWireless Controllers, you must ensure that controllers are discovered using an SNMPv2c or SNMPv3 profile. The profile must also contain SSH CLI credentials for the controller. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers. 2. Verify that the following ports are accessible through firewalls for the Extreme Management Center Server and Wireless Controllers to communicate: SSH: 22 SNMP: 161, 162 Langley: 20506