Extreme Networks ®

Extreme Suite-Wide Tools 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. <u>DEFINITIONS</u>. "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. <u>TERM</u>. 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. <u>GRANT OF SOFTWARE LICENSE</u>. 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. <u>LICENSE TYPES</u>.

   - *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. <u>AUDIT RIGHTS</u>. 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. <u>RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS</u>. 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. <u>TITLE AND PROPRIETARY RIGHTS</u>

   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. <u>PROTECTION AND SECURITY</u>. 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. <u>UNITED STATES GOVERNMENT RESTRICTED RIGHTS</u>. 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. <u>LIMITED WARRANTY AND LIMITATION OF LIABILITY</u>. 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. <u>JURISDICTION</u>. 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. <u>GENERAL</u>.

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® Suite-Wide Tools

This folder contains Help topics describing the following suite-wide tools and features that are available from all Extreme Management Center applications:

- **Authorization/Device Access** -- This tool lets you define SNMP *credentials* used to access your network devices, and create *profiles* that use these credentials for various device access levels. You can access this tool from the Tools menu in any application.

- **Command Script Tool** -- This tool lets you execute a sequence of CLI commands (a script) on a set of devices. This can be useful for many purposes, such as modifying a number of device configurations at one time.

- **ExtremeNetworks.com Update** -- This tool provides an easy way to access and download product updates using a web update operation. You can access web update from the Help menu in any application.

- **Event View** -- The Extreme Management Center Event View (located at the bottom of the Extreme Management Center Console main window) lets you view alarm, event, and trap information for Extreme Management Center and other Extreme Management Center applications.

- **LDAP Configuration** -- Define the LDAP configurations used in your Extreme Management Center applications.

- **Extreme Management Center Failover** -- A Extreme Management Center server recovery plan for the Extreme Management Center virtual appliance using the VMware ESX High Availability (HA) feature.

- **Extreme Management Center Help** -- All Extreme Management Center documentation is available in this online help system. Learn how to access Help for Extreme Management Center applications and use the Help Search capability.

- **Extreme Management Center Services** -- When you install Extreme Management Center, you have the option of enabling the Extreme Management Center Services. This Help topic provides information on enabling the Extreme Management Center Services and using the Services Manager.

- **Options** -- Set suite-wide options using the Options window accessed from the Tools menu in any application.

- **RADIUS Configuration** -- Define the RADIUS servers used in your Extreme Management Center applications.

- **Server Information** -- This tool lets you view and configure certain Extreme Management Center Server functions, including client connections, database properties, database backup and restore, locks, and licenses. You can access this tool from the Tools menu in any application.

- **Table Tools --** Many Extreme Management Center tables provide tools that let you customize table settings and help you to find, filter, sort, print, and export information in tables.

- **Troubleshooting** -- Provides a list of items to check when certain Extreme Management Center functionality is not performing as expected.

Document Version

The following table displays the revision history for the Suite-Wide Tools Help documentation.

Date	Revision Number	Description
3-18	8.1 Revision -00	Extreme Management Center 8.1 release
04-16	7.0 Revision -00	Extreme Management Center 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release

PN: 9035434

Authorization/Device Access (Legacy)

Use the Authorization/Device Access tool to configure SNMP credentials and user access privileges for your Extreme Management Center applications. You can access this tool from the **Tools > Authorization/Device Access** menu option in any application.

The Authorization/Device Access tool has four tabs:

- Users/Groups tab lets you manage user access to specific features and capabilities.
- Profiles/Credentials tab lets you define SNMP *credentials* used to access your network devices, and create *profiles* that use these credentials for various device access levels.
- Profile/Device Mapping tab lets you specify the *profiles* that will be used when communicating with network devices.
- Manage SNMP Passwords tab where you can manage the *credentials* that have been set on your network's devices.

How to Configure Profile/Device Mapping in Extreme Management Center (Legacy)

Use the **Profile/Device Mapping** tab to specify which profile is used by each Authorization Group when communicating with a specific device. The Read credential of the Extreme Management Center Administrator profile is used for device Discovery and status polling. All other SNMP communications use the profiles specified here.

Assigning Profiles to Devices

Devices selected in the left (tree) panel appear in the table in the right panel together with the current profile assignments associated with each Authorization Group. The Table Editor button activates the editing row where specific profile selections can be made.

To assign profiles:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profile/Device Mapping** tab in the **Authorization/Device Access** window.

2. Select one or more devices or device groups in the left (tree) panel.

3. Select one or more rows (devices) in the table and click **Table Editor** ([icon]) button.

4. Click in the Table Editor Row (at the bottom of the table) for the Authorization Group you are configuring and select a profile from the drop-down menu.

5. Repeat steps 3 and 4 until you have finished assigning profiles.

NOTE: The *NetSight (Extreme Management Center) Administrator* column shows the profile used by the Extreme Management Center Administrator group. The profile listed/selected for each Authorization Group column is 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.

---

6. Click [icon] (**Apply**) to set the selected profiles for your Authorization Groups/devices.

Related Information

For information on related windows:

- [Manage SNMP Passwords Tab](#)
- [Users/Groups Tab](#)
- [Profile/Device Mapping Tab](#)
- [Profiles/Credentials Tab](#)

For information on related tasks:

- [How to Manage Users and Groups](#)
- [How To Configure Profiles and Credentials](#)
- [How to Manage SNMP Passwords](#)

How to Configure Profiles and Credentials in Extreme Management Center (Legacy)

Use the Profiles/Credentials tab to define 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. Extreme Management Center applications need access to devices in order to control certain device functions and retrieve information for device properties views, FlexViews and periodic polling. 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 specific devices in the Profile/Device Mapping tab.

Instructions for:

- Managing SNMP Credentials
    - Create SNMP Credential
    - Edit SNMP Credential
    - Delete SNMP Credential
- Managing CLI Credentials
    - Create CLI Credential
    - Edit CLI Credential
    - Delete CLI Credential
- Managing Profiles
    - Create Profile
    - Edit Profile
    - Delete Profile

Managing Credentials

Credentials define the authentication values (for example, user names and passwords) used to access your network devices.

- **SNMP Credentials** provide support for device management using SNMP.
- **CLI Credentials** provide support for device management using the command line interface (CLI).

SNMP Credentials

To create an SNMP credential:

1. Click ⬛ or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the SNMP Credentials subtab, and click **Add Credential**. The Add Credential window opens.

3. Type a name (up to 32 characters) for your new credential and select an SNMP version. If you select SNMPv1 or SNMPv2, the window lets you enter a community name as the password for this credential. If you select SNMPv3, you can specify passwords for Authentication and Privacy.

   SNMPv1/SNMPv2:

   a. Type a community name into the **Community Name** field.

   SNMPv3:

   a. Type a user name into the **User Name** field. This is the User Name used for device access.

   b. Select an **Authentication Type** (MD5, SHA1, or None).

   c. Type the same password (between 1 and 64 characters in length) into both the **Authentication Password** and the **Confirm Password** fields. The password fields are disabled when the Authentication Type is set to **None**.

   d. Select a **Privacy Type** (DES or None). Privacy settings are disabled when the Authentication Type is set to **None**.

   e. Type the same password (between 1 and 64 characters in length) into both the **Privacy Password** and the **Confirm Password** fields. The password fields are disabled when the Privacy Type is set to **None**.

4. Click **Apply**. You can add another credential or click **Close** to dismiss the Add Credential window. Your new credential appears in the SNMP Credentials table.

To edit an SNMP credential:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the SNMP Credentials subtab, and select the credential that you want to edit from the SNMP Credentials table.

3. Click **Edit**. The Edit Credential window opens where you can modify the settings for the selected credential.

4. Type a name (up to 32 characters) for your new credential and select a SNMP version. If you select SNMPv1 or SNMPv2, the window accommodates entering a community name as the password for this credential. If you select SNMPv3, you can specify passwords for Authentication and Privacy.

   SNMPv1/SNMPv2:

   a. Type a community name into the **Community Name** field.

   SNMPv3:

   a. Type a user name into the **User Name** field. This is the User Name used for device access.

   b. Select an **Authentication Type** (MD5, SHA1, or None).

   c. Type the same password (between 1 and 64 characters in length) into both the **Authentication Password** and the **Confirm Password** fields. The password fields are disabled when the Authentication Type is set to **None**.

   d. Select a **Privacy Type** (DES or None). Privacy settings are disabled when the Authentication Type is set to **None**.

   e. Type the same password (between 1 and 64 characters in length) into both the **Privacy Password** and the **Confirm Password** fields. The password fields are disabled when the Privacy Type is set to **None**.

5. Click **Apply** and **Close**. The changes to the selected credential appear in the SNMP Credentials table. If the settings are changed for a credential that is currently being used with a profile that is applied to one or more devices, a confirmation dialog is opened to determine how the changes will be handled. You will be asked if you want to change the password on the device(s). You can then select the devices where the password will be changed and, if this user is a valid user on the device(s), then the new password will be set on the device.

To delete an SNMP credential:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the SNMP Credentials subtab, and select the credential that you want to delete from the SNMP Credentials table.

3. Click **Delete**. The selected credential is removed from the table.

CLI Credentials

> **NOTE:** When configuring CLI Credentials for ExtremeWireless Controllers, you must add the username and password Login credentials for the controller to the 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.

To create a CLI credential:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the CLI Credentials subtab, and click **Add**. The Add Credential window opens.

3. Specify the user name and passwords for the credential.

4. Select the type of connection for the credential: SSH or Telnet.

5. Click **OK**. Your new credential appears in the CLI Credentials table.

To edit a CLI credential:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the CLI Credentials subtab, and select the credential that you want to edit from the CLI Credentials table.

3. Click **Edit**. The Edit Credential window opens where you can modify the settings for the selected credential.

4. Click **OK**. The changes to the selected credential appear in the CLI Credentials table.

To delete a CLI credential:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. Select the CLI Credentials subtab, and select the credential that you want to delete from the CLI Credentials table.

3. Click **Delete**. The selected credential is removed from the table.

Managing Profiles

Profiles are assigned to device models in the Extreme Management Center database. They identify the credentials that are used for the various access levels when communicating with the device.

NOTE: When configuring profiles for ExtremeWireless Controllers, you must make sure that 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.

To create a profile:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. In the Device Access Profiles table, click **Add Profile**. The Add Profile window opens.

3. Type a name (up to 32 characters) for your new profile and select an SNMP version. If you select SNMPv1 or SNMPv2, you can select credentials for Read, Write, and Max Access. If you select SNMPv3, you can select credentials and security levels for Read, Write, and Max Access.

4. Select the CLI Credential for this profile. CLI credentials provide support for management of devices using the command line interface (CLI).

5. Click **Apply**. You can add another profile or click **Close** to dismiss the Add Profile window. Your new profile(s) appears in the Device Access Profiles table.

To edit a profile:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. In the Device Access Profiles table, select the profile that you are editing.

3. Click **Edit**. The Edit Profile window opens where you can modify the settings for the selected profile.

4. Click **Apply** and **Close**. The changes to the selected profile appear in the Device Access Profiles table.

To delete a profile:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Profiles/Credentials** tab in the **Authorization/Device Access** window.

2. In the Device Access Profiles table, select the profile that you are deleting.

3. Click **Delete**. The selected profile is removed from the table.

Related Information

For information on related windows:

- Users/Groups Tab
- Profile/Device Mapping Tab
- Profile/Device Mapping Tab
- Manage SNMP Passwords Tab

For information on related tasks:

- How to Manage Users and Groups
- How To Configure Profile/Device Mapping
- How to Manage SNMP Passwords

How to Configure User Access to Extreme Management Center Applications (Legacy)

This Help topic describes the steps for configuring the authentication and authorization process that provides access for Extreme Management Center users. When you install Extreme Management Center, the user performing the installation is automatically created as an Authorized User with Extreme Management Center Administrator capabilities. This administrative user is capable of creating additional Extreme Management Center users and assigning their access levels.

The **Users and Groups** tab of the Authorization/Device Access tool is where you will define the method that will be 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 or the NAC Manager Dashboard. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication. Steps for configuring each of these methods are provided below.

The tab is also used 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. 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.

NOTE: When changes to authentication and authorization configurations are made, clients must be restarted in order to be subject to the new configuration. It is suggested that you disconnect those clients affected by the changes made to your authentication and authorization configurations. You can use the Client Connections tab in the Server Information window to help identify which clients are affected by the changes, and disconnect those clients.

Use the instructions below for configuring authentication and authorization based on the authentication method appropriate for your network.

Instructions for configuring:

- [OS Authentication](#)

- [LDAP Authentication](#)

- [RADIUS Authentication](#)

OS Authentication

OS Authentication is the default authentication method, where the Extreme Management Center Server uses the underlying host operating system to authenticate users. Use the following instructions to configure the OS authentication method and set up your users and authorization groups.

NOTE: You must have user accounts created for your Extreme Management Center users in the underlying operating system. For Windows operating systems, access your Windows OS Help to determine the appropriate steps for adding a user account. For Linux operating systems, from the command line use the useradd and passwd commands to add a user account.

---

1. Click the [icon] toolbar button, or select **Authorization/Device Access** from the **Tools** menu. The Authorization/Device Access window opens with the [Users/Groups tab](#) selected.

2. **Create your Authorization Groups.**

   a. In the Authorized Groups section, click **Add Group**. The [Add Group](#) window opens where you can define the capabilities for the new group.

   b. Enter a name for your new group in the Authorization Group Name field.

   c. Do not enter anything in the Membership Criteria field.

   d. Select the **Capabilities** tab and expand the tree, and select the capabilities granted to users that are members of this group. See [Authorization Group Capabilities](#) for an explanation of each capability.

   e. Select the **Settings** tab and choose a SNMP Redirect option for members of this group:

      - **Allow Users to Configure SNMP Redirect in Options** - lets users edit the Suite-wide Option setting for Client/Server SNMP Redirect.

      - **Always Redirect SNMP to the Extreme Management Center (NetSight) Server** - all SNMP requests always go through the server.

      - **Never Redirect SNMP to the Extreme Management Center (NetSight) Server** - SNMP requests are always made from the client system.
      These settings have no effect when both the client and server are running on

the same system.

f. Click **Apply** to confirm your selections and **Close** to dismiss the Add Group window.

g. Your new group now appears in the Authorization Groups table.

3. **Create a list of authorized users.**

a. In the Authorized Users section, click **Add User**. The Add User window opens where you can define a new Authorized User and assign it a group membership.

b. Enter the user's name and the domain/hostname that will be used to authenticate.

c. Select the authorization group to which to add the current user.

d. Click **Apply** to confirm your selections and **Close** to dismiss the Add User window.

e. The new user now appears in the Authorized Users table.

4. **Specify your authentication method.**

a. In the User Authentication section, select the Default (OS Authentication) Authentication Method.

b. If desired, enable Automatic Membership and specify an authorization group. The Automatic Membership feature allows a user who has not been manually added to the Authorized Users table to be authenticated by the operating system, and dynamically added to the table and assigned to the specified authorization group the first time that they log in. These users are indicated by a "Yes" in the Automatic Member column of the Authorized Users table.

5. Changes made to the Users/Groups tab are automatically saved to the Extreme Management Center Database.

LDAP Authentication

With LDAP authentication, the Extreme Management Center Server uses the specified LDAP configuration to authenticate users. You can configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, you could create an authorization group that matches everyone in a particular organization, department, or location. Use the following instructions to configure the LDAP authentication method and set up your users and authorization groups.

1. Click the [icon] toolbar button, or select **Authorization/Device Access** from the **Tools** menu. The Authorization/Device Access window opens with the <u>Users/Groups tab</u> selected.

2. **Create your Authorization Groups.** When a user authenticates using LDAP authentication, the attributes associated with that user are matched against a list of criteria specified as part of each authorization group. The first group listed in the table that includes a criteria that matches 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.
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 will not be authenticated and will not be allowed to log in. For this reason, it is recommended to create a "catch-all" group (for example, objectClass=person), whose criteria is very generic and whose capabilities are highly restricted. This will help differentiate between a user who cannot authenticate successfully, and a user who does not belong to any group.

   a. In the Authorized Groups section, click **Add Group**. The <u>Add Group</u> window opens where you can define the capabilities for the new group.

   b. Enter a name for your new group in the Authorization Group Name field.

   c. Enter the Membership Criteria that will be used to match against user attributes to determine group membership. The criteria is entered as name=value pairs, for example, department=IT. 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: You cannot define membership criteria for the Extreme Management Center Administrator Group. Membership in the administrator group must be assigned manually using the Authorized Users table.

   d. Select the **Capabilities** tab and expand the tree, and select the capabilities granted to users that are members of this group. See <u>Authorization Group Capabilities</u> for an explanation of each capability.

   e. Select the **Settings** tab and choose a SNMP Redirect option for members of this group:

- **Allow Users to Configure SNMP Redirect in Options** - lets users edit the Suite-wide Option setting for Client/Server SNMP Redirect.

- **Always Redirect SNMP to the Extreme Management Center (NetSight) Server** - all SNMP requests always go through the server.

- **Never Redirect SNMP to the Extreme Management Center (NetSight) Server** - SNMP requests are always made from the client system.
These settings have no effect when both the client and server are running on the same system.

   f. Click **Apply** to confirm your selections and **Close** to dismiss the Add Group window.

   g. The new group is listed in the table. Use the **Move Up** and **Move Down** buttons to adjust the group's position in the table, keeping in mind that users are assigned group membership based on the first group listed in the table that they match.

3. **Create a list of authorized users.** You only need to do this if you want to manually create special users that will authenticate using OS Authentication and be assigned membership in the Extreme Management Center Administrator Group or another authorization group.

   a. In the Authorized Users section, click **Add User**. The [Add User](#) window opens where you can define a new Authorized User and assign it a group membership.

   b. Enter the user's name and the domain/hostname that will be used to authenticate.

   c. Select an authorization group where this user will be a member.

   d. Click **Apply** to confirm your selections and **Close** to dismiss the Add User window.

   e. The new user now appears in the Authorized Users table.

4. **Specify your authentication method.**

   a. Select the LDAP Authentication Method.

   b. Use the drop-down list to select the LDAP configuration for the LDAP server on your network that you want to use to authenticate users. Use the configuration menu button ⏷ (to the right of the drop-down list) to add or edit an LDAP configuration, or manage your LDAP configurations.

c. If desired, enable **Authenticate to OS on LDAP failure** and specify an authorization group. This feature provides the option to use OS Authentication Automatic Membership if the LDAP authentication should fail for any reason. Automatic Membership allows a user who has not been manually added to the Authorized Users table to be authenticated by the operating system, and dynamically added to the table and assigned to the specified authorization group the first time that they log in. These users are indicated by a "Yes" in the Automatic Member column of the Authorized Users table.

> **NOTE:** If LDAP authentication should fail for any reason, and the **Authenticate to OS on LDAP failure feature** in **not** enabled, users that have been manually added to the Authorized Users table will still have permission to log in.

5. Changes made to the Users/Groups tab are automatically saved to the Extreme Management Center Database.

RADIUS Authentication

With RADIUS authentication, the Extreme Management Center Server uses the specified RADIUS servers to authenticate users. You can configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. Use the following instructions to configure the RADIUS authentication method and set up your users and authorization groups.

> **NOTE:** The RADIUS Authentication mode supports the PAP authentication type.

1. Click the [icon] toolbar button, or select **Authorization/Device Access** from the **Tools** menu. The Authorization/Device Access window opens with the Users/Groups tab selected.

2. **Create your Authorization Groups.** When a user authenticates using RADIUS authentication, the attributes associated with that user are matched against a list of criteria specified as part of each authorization group. The first group listed in the table that has a criteria that matches 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.
   A user whose attributes don't match any of the criteria specified for any of the groups will not be authenticated and will not be allowed to log in. For this reason, it is recommended to create a "catch-all" group whose criteria is very generic and

whose capabilities are highly restricted. This will help differentiate between a user who cannot authenticate successfully, and a user who does not belong to any group.

a. In the Authorized Groups section, click **Add Group**. The Add Group window opens where you can define the capabilities for the new group.

b. Enter a name for your new group in the Authorization Group Name field.

c. Enter the Membership Criteria that will be used to match against user attributes to determine group membership. The criteria is entered as name=value pairs, for example, Service-Type=Framed-User. 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:** You cannot define membership criteria for the Extreme Management Center Administrator Group. Membership in the administrator group must be assigned manually using the Authorized Users table.

d. Select the **Capabilities** tab and expand the tree, and select the capabilities granted to users that are members of this group. See Authorization Group Capabilities for an explanation of each capability.

e. Select the **Settings** tab and choose a SNMP Redirect option for members of this group:

- **Allow Users to Configure SNMP Redirect in Options** - lets users edit the Suite-wide Option setting for Client/Server SNMP Redirect.

- **Always Redirect SNMP to the ECC (NetSight) Server** - all SNMP requests always go through the server.

- **Never Redirect SNMP to the Extreme Management Center (NetSight) Server** - SNMP requests are always made from the client system.

These settings have no effect when both the client and server are running on the same system.

f. Click **Apply** to confirm your selections and **Close** to dismiss the Add Group window.

g. The new group will be listed in the table. Use the **Move Up** and **Move Down** buttons to adjust the group's position in the table, keeping in mind that users

are assigned group membership based on the first group listed in the table that they match.

3. **Create a list of authorized users.** You will only need to do this if you want to manually create special users that will authenticate using OS Authentication and be assigned membership in the Extreme Management Center Administrator Group or another authorization group.

   a. In the Authorized Users section, click **Add User**. The Add User window opens where you can define a new Authorized User and assign it a group membership.

   b. Enter the user's name and the domain/hostname that will be used to authenticate.

   c. Select an authorization group where this user will be a member.

   d. Click **Apply** to confirm your selections and **Close** to dismiss the Add User window.

   e. The new user now appears in the Authorized users table.

4. **Specify your authentication method.**

   a. Select the RADIUS Authentication Method.

   b. Use the drop-down list to select the primary RADIUS server and backup RADIUS server (optional) on your network that you want to use to authenticate users. Use the configuration menu button ⌄ (to the right of the drop-down list) to add or edit a RADIUS server, or manage your RADIUS servers.

   c. If desired, enable **Authenticate to OS on RADIUS failure** and specify an authorization group. This feature provides the option to use OS Authentication Automatic Membership if the RADIUS authentication should fail for any reason. Automatic Membership allows a user who has not been manually added to the Authorized Users table to be authenticated by the operating system, and dynamically added to the table and assigned to the specified authorization group the first time that they log in. These users are indicated by a "Yes" in the Automatic Member column of the Authorized Users table.

   NOTE: If RADIUS authentication should fail for any reason, and the **Authenticate to OS on RADIUS failure feature** in **not** enabled, users that have been manually added to the Authorized Users table will still have permission to log in.

   ---

5. Changes made to the Users/Groups tab are automatically saved to the Extreme Management Center Database.

Related Information

For information on related windows:

- Manage SNMP Passwords Tab
- Users/Groups Tab
- Profile/Device Mapping Tab
- Profiles/Credentials Tab

For information on related tasks:

- How To Configure Profiles and Credentials
- How To Configure Profile/Device Mapping
- How to Manage SNMP Passwords

How to Manage SNMP Passwords in Extreme Management Center (Legacy)

Use this tab to collectively manage the credentials that have been set on your network's devices.

Instructions for:

- [Setting SNMPv1/2 Credentials](#)
- [Setting SNMPv3 Credentials](#)

Setting SNMPv1/2 Credentials

When a SNMPv1 or SNMPv2 credential is selected from the drop-down list above the table, the table lists the devices where that credential is set and you can define a *New Community Name* for access to the devices in the table.

To set SNMPv1 or SNMPv2 credentials on your devices:

1. Click ![icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Manage SNMP Passwords** tab in the **Authorization/Device Access** window.

2. Select an SNMPv1 or SNMPv2 credential from the Credential drop-down list. The table will list all of the devices where the selected credential can be used.

3. Type the new community name that you want to set on the devices listed in the table.

4. Click **Test** to verify that the credential in the "Use for Set" column can access the applicable MIBs on the device.

5. If the **Test Results** are acceptable, click **Apply** to set the community name on the devices.

Setting SNMPv3 Credentials

When an SNMPv3 credential is selected, you can define a new *Authentication* password and *Privacy* password for access to the devices in the table.

To set an SNMPv3 credential on your devices:

1. Click [icon] or choose **Authorization/Device Access** from the **Tools** menu. Select the **Manage SNMP Passwords** tab in the **Authorization/Device Access** window.

2. Select an SNMPv3 credential from the **Credential** drop-down menu. The table lists all of the devices where the selected credential can be used.

3. Type the new Authentication and Privacy passwords that you want to set on the devices listed in the table.

4. Click **Test** to verify that the credential in the "Use for Set" column can access the applicable MIBs on the device.

5. If the **Test Results** are acceptable, click **Apply** to set the passwords on the devices.

Test Button

This button lets you test to verify that the credential in the "Use for Set" column can access the applicable MIBs on the device.

Apply Button

Sets your credential changes on the devices in the table.

Related Information

For information on related windows:

- Manage SNMP Passwords Tab
- Users/Groups Tab
- Profile/Device Mapping Tab
- Profiles/Credentials Tab

For information on related tasks:

- How to Manage Users and Groups
- How To Configure Profiles and Credentials
- How To Configure Profile/Device Mapping

Authorization Group Capabilities (Legacy)

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 using the Users and Groups tab in the Authorization/Device Access tool, accessed from the Tools menu in any Extreme Management Center application. In the Add/Edit Group window, the Capabilities tab lists all the various capabilities for your selection. The capabilities are divided into suite-wide and application-specific capabilities. Checking a capability in the tree grants access to that capability.

See below for a description of each capability.
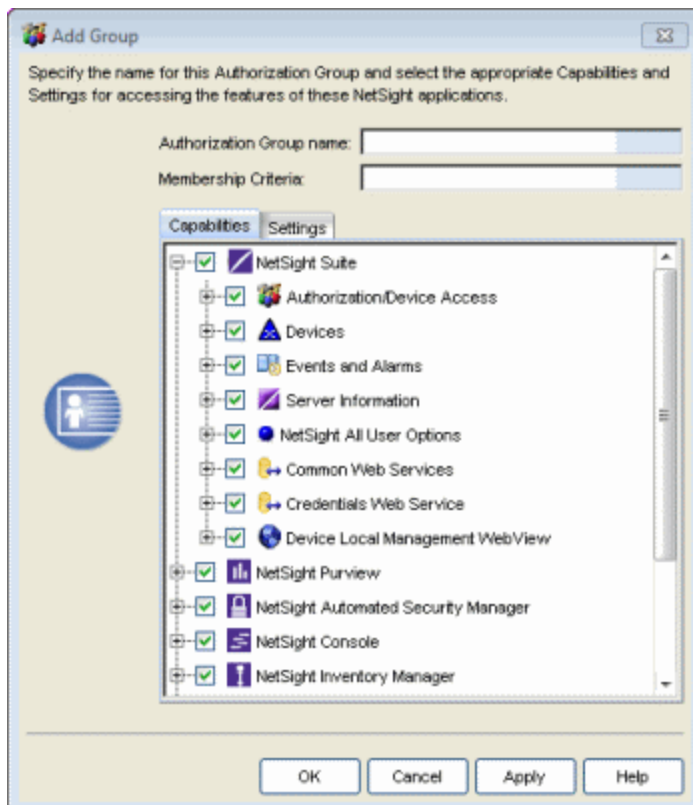
The following sections provide a description of each capability:

- Extreme Management Center Suite
    - Authorization/Device Access
    - Devices
    - Events and Alarms
    - Server Information
    - Extreme Management Center All User Options
    - Common Web Services
    - Credentials Web Service
    - Device Local Management WebView
- Extreme Management Center Application Analytics
- Extreme Management Center Console
    - Wireless Manager
    - VLAN Models
- Extreme Management Center Mediation Agent
- Extreme Management Center Policy Manager
- Extreme Management Center NAC Manager
- Extreme Management Center OneView

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, which can be 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.

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.

Server Information

View Server Information

Allows the ability to view, but not to configure the Server Information tool, which can be 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.

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.

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 Control engines without requiring a login, as long as the user has the necessary credentials. Users who do not have this capability are required to log in.

Auto Login to Web Local Management for ExtremeWireless Wireless Controllers

Allows the ability to launch local management for wireless controllers without requiring a login, as long as the user has the necessary credentials. Users who do not have this capability are required to log in.

Extreme Management Center Application Analytics

Application Analytics Read Access

Allows the ability to access the OneView **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 OneView **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 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 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 NAC Manager

Launch NAC Manager
> Allows the ability to launch the NAC Manager application. Users who do not have this capability will 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 OneView application but does not provide any OneView report access. Selecting only this capability without any other OneView capabilities would be the same as not allowing OneView access.

Access OneView Reports

> Adds the ability to view all OneView reports accessed from the **Reports** tab.

Access OneView Search

> Adds the ability to use the OneView **Search** tab.

Access OneView Administration

> Adds the ability to access OneView administration tools and enable data collection.

NetFlow Read Access

> Adds the ability to view the OneView **Flows** tab.

Maps

Allows the ability to perform the following OneView map functions:

- Maps Read Access - Adds the ability to access the OneView **Map** tab and view the maps.

- Maps Read/Write Access - Adds the ability to access the OneView 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 OneView 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 OneView Identity and Access 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 OneView NetSight (Extreme Management Center) Manager.

NOTE: Access to some OneView components is determined by capabilities in other capabilities groups:

NetSight (Extreme Management Center) Console > Wireless Manager > Launch
Adds the ability to view the OneView **Wireless** tab.

NetSight (Extreme Management Center) Suite > Devices > Add, Discover and Import
Adds the ability to add devices in the OneView **Network** tab.

NetSight (Extreme Management Center) Suite > Devices > Delete
Adds the ability to delete devices in the OneView **Network** tab.
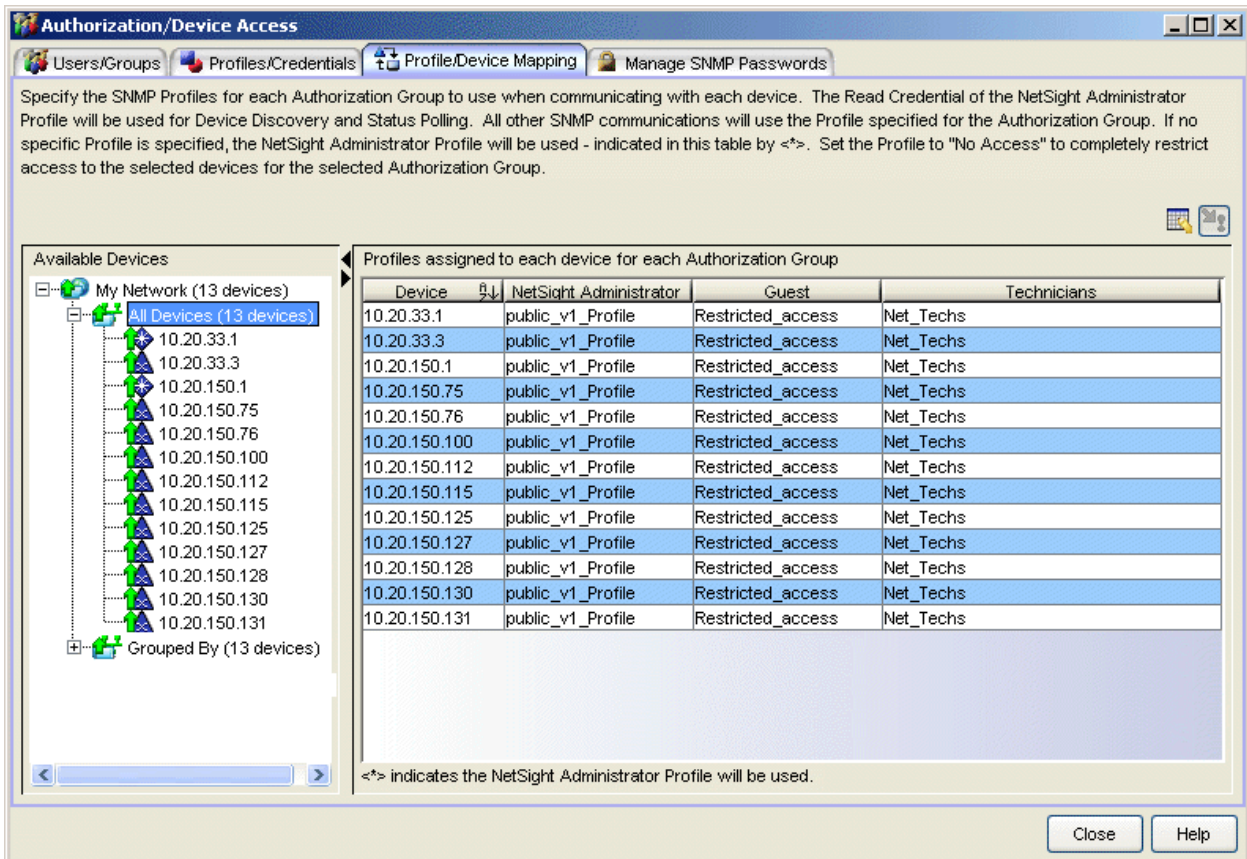
Inventory Manager > Configuration Archive Management > View/Compare Configurations
Adds the ability to compare archived device configurations in either the OneView **Network** tab or the Archive Details Report available in the OneView **Reports** tab.

Profile/Device Mapping Tab (Legacy)

This tab lets you define the specific Profiles to be used by users in each Authorization Group when communicating with network devices. The view consists of 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. The Table Editor button 🖼 activates the editing row where profile selections are made.

Device Tree

The left panel contains a device tree, where you select the devices you want 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 have 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.

Table Editor Row

This row is visible when the Show/Hide Table Editor button is toggled to make the Table Editor visible. The drop down list for each Authorization Group column contains all of the Profiles that have been created in the Extreme Management Center database, including *Ping Only, No Access*, and the profile selected on the Profiles/Credentials tab as the *Default* profile. Selecting a profile in the Table Editor row alters the value for that entry in the row(s) selected in the table. Once you select a profile to be changed for your selected column(s), a green exclamation mark (!) marks the cells that have been changed (but not Applied) and the Apply button becomes active. Clicking the (Show/Hide Table Editor button) at this point cancels your changes, restores the original profiles, and hides the Table Editor.

Clicking Apply sets the profiles that you've changed for the selected devices, removes the !, and hides the Table Editor row.

Show/Hide Table Editor

This button toggles the Table Editor, a row at the bottom of the table that allows you to define a profile for each Authorization Group. Use the drop down list to select a profile for each group, and then click Apply.

Apply Button

This button is active when the Table Editor is enabled. Apply sets your profile selections for the Authorization Groups, clears the ! from the table, and hides the table editor row.

Related Information

For information on related windows:

- [Users/Groups Tab](#)
- [Profiles/Credentials Tab](#)
- [Manage SNMP Passwords Tab](#)

For information on related tasks:

- [How to Manage SNMP Passwords](#)
- [How to Configure Profiles and Credentials](#)
- [How to Configure Profile/Device Mapping](#)
- [How to Manage Users and Groups](#)

Profiles/Credentials Tab (Legacy)

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.

- **Credentials** - Credentials define the authentication values (for example, user names and passwords) that will be used to access your network devices.

    - **SNMP Credentials** provide support for device management using SNMP.

    - **CLI Credentials** provide support for device management using the command line interface (CLI).

- **Profiles** - Profiles are assigned to device models in the Extreme Management Center database. They identify the credentials that are used for the various access levels when communicating with the device.

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 specific devices in the Profile/Device Mapping tab.
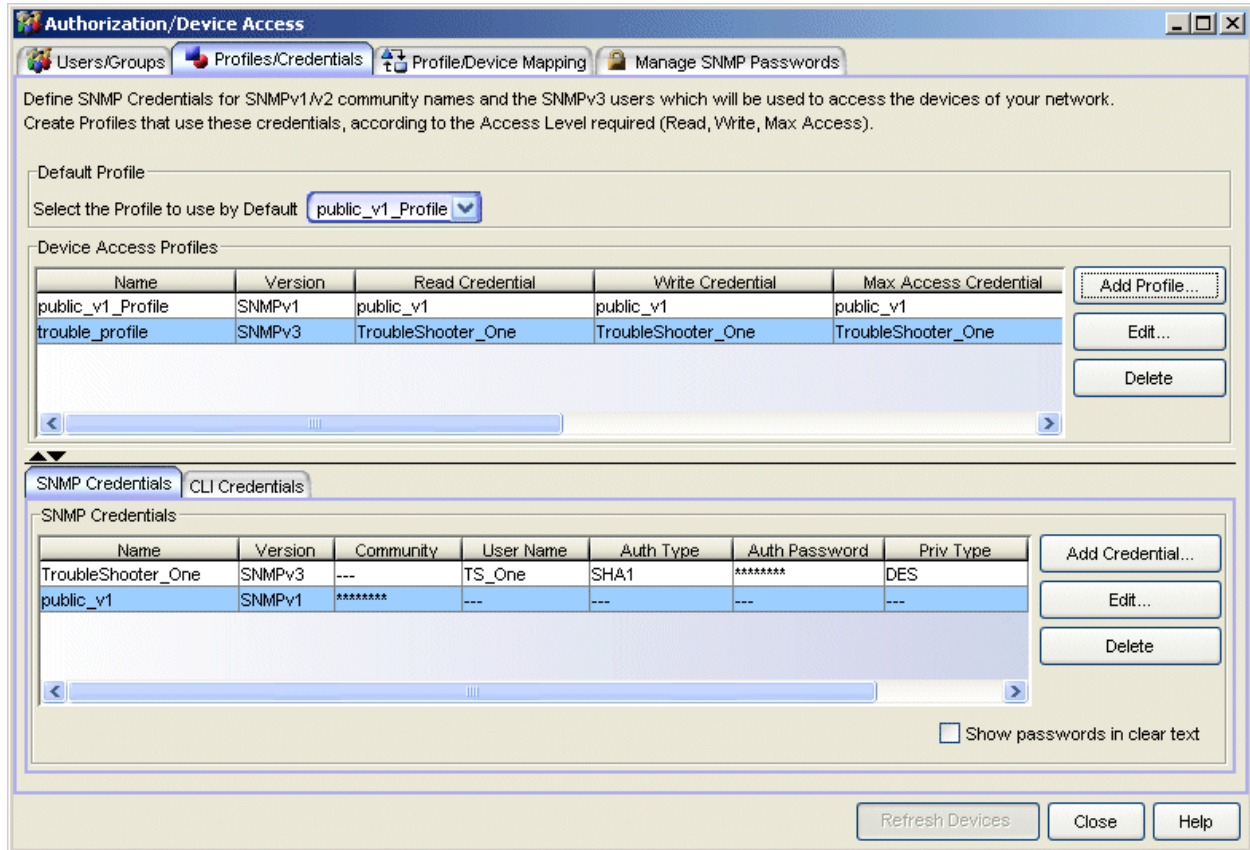
Default Profile

This drop-down list lets you specify a profile used by default to access a device.

Default Access Profiles Table

This table lists all of the profiles created. The public_v1_Profile is automatically created during Console installation and cannot be deleted.

Name

This is the name assigned when the profile is created.

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 SNMPv1 or SNMPv2c, these columns do not apply. When the **Version** is SNMPv3, these columns contain the security level specified for each access credential.

CLI Credential

The CLI credential specified for the profile.

Add Profile Button

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

Edit (Profile) Button

Opens the Edit Profile window where you can modify the SNMP version and passwords/community names used by a selected profile.

Delete (Profile) Button

Removes the selected Profile from the Device Access Profiles table. You cannot delete the profile that is currently selected to be the **Default Profile**.

SNMP Credentials Subtab

This tab lists all of the SNMP credentials that have been created in the Extreme Management Center database. The public_v1 credential is automatically created during Extreme Management Center installation and cannot be deleted.

Name

This column lists names assigned to credentials that have been created in the Extreme Management Center database.

Version

This is the SNMP protocol version for the credential. Credentials can be configured for **SNMPv1**, **SNMPv2c**, or as **SNMPv3**.

Community

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.

Auth Type/Auth Password, Priv Type/Priv Password

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.

Show passwords in clear text

> When this option is checked, passwords and community names appear as text. The default setting for this option is unchecked, and passwords and community names appear as a string of asterisks.

Add Credential Button

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

Edit (Credential) Button

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

Delete (Credential) Button

> Removes a selected credential from the SNMP Credentials table.

CLI Credentials Subtab

> This tab lists all of the CLI credentials that have been created in the Extreme Management Center database. The Default and <No Access> credentials are created automatically during Extreme Management Center installation and cannot be deleted.

User Name

> The User Name used for device access.

Description

> A description of the CLI credential.

Type

> The communication protocol used for the connection (SSH or Telnet).

Add (CLI Credential) Button

> Opens the Add Credential window where you can define a new CLI credential.

Edit (CLI Credential) Button

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

Delete (CLI Credential) Button

> Removes a selected credential from the CLI Credentials table.

Add/Edit Profile Window

This window lets you define the SNMP and CLI Credentials for a new profile or modify the credentials for an existing profile.

> **NOTE:** When configuring profiles for ExtremeWireless Controllers, you must make sure that controllers are discovered using an SNMPv2c or SNMPv3 profile. This profile must also contain SSH CLI credentials for the controller. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers.

Profile Name

A unique name (up to 32 characters) that you assign 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

The Read, Write, Max Access define the community names used for these levels of access.

- **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

The Read, Write, Max Access levels are defined by Credentials and Security Level:

Credentials

Credential Names are assigned to each of the three SNMPv3 access levels that are used for the Read, Write and Max Access operations.

- **Read** - used for read operations (*gets*).
- **Write** - used for write operations (*sets*).
- **Max Access** - used for write operations (*set*) that require administrative access.

Security Level

Each access level can be assigned a security level:

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

CLI Credential

Use the drop-down list to select the CLI Credential for this profile. CLI credentials provide support for device management using the command line interface (CLI).

Add/Edit SNMP Credential Window

This window lets you define or edit the names and community names/passwords for SNMP credentials.

Credential Name

A unique name (up to 32 characters) that you assign 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 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 Type

For SNMPv3 credentials, select **MD5**, **SHA1,** or **None**, from this drop-down list .

Specify/Confirm Password

This is the password (between 1 and 64 characters in length) that will be used to determine Authentication. These fields are disabled for Authentication Type, **None**. If an existing password is changed and the credential is currently used with a profile that is applied to one or more devices, a confirmation dialog is opened to determine how the changes will be handled. You will be asked if you want to change the password on the device(s). You can then select the devices where the password will be changed and, if this user is a valid user on the device(s), then the new password will be set on the device.

Privacy Type

For SNMPv3 credentials, select **DES** or **None** from this drop-down list. These settings are disabled if Authentication Type **None** is selected.

Specify/Confirm Password

This is the password (between 1 and 64 characters in length) that will be used to determine Privacy. These fields are disabled for Privacy Type, **None**. If an existing password is changed and the credential is currently used with a profile that is applied to one or more devices, a confirmation dialog is opened to determine how the changes will be handled. You will be asked if you want to change the password

on the device(s). You can then select the devices where the password will be changed and, if this user is a valid user on the device(s), then the new password will be set on the device.

Show passwords in clear text
> When this option is checked, passwords and community names appear as text. The default setting for this option is unchecked and passwords and community names appear as a string of asterisks.

Add/Edit CLI Credential Window

This window lets you define or edit the user name and passwords for a CLI credential.

User Name
> The User Name used for device access.

Description
> A description of the credential.

Passwords

The passwords used to determine different levels of access to the device:

- Login - The password required to start a CLI session.

- Enable - The password for entering Enable mode.

- Configuration - The password for entering Configure mode.

NOTE: When configuring CLI Credentials for ExtremeWireless Wireless 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.

Type

The communication protocol used for the connection (SSH or Telnet).

Show passwords in clear text

When this option is checked, passwords appear as text. The default setting for this option is unchecked and passwords appear as a string of asterisks.

Related Information

For information on related windows:

- [Users/Groups Tab](#)
- [Profile/Device Mapping Tab](#)
- [Manage SNMP Passwords Tab](#)

For information on related tasks:

- [How to Manage SNMP Passwords](#)
- [How to Configure Profiles and Credentials](#)
- [How to Configure Profile/Device Mapping](#)
- [How to Manage Users and Groups](#)

Users/Groups Tab (Legacy)

The Users/Groups tab is where you define the method that will be used to authenticate users who are attempting to launch an Extreme Management Center client or access the Extreme Management Center database using the Extreme Management Center Server Administration web page or the NAC Manager Dashboard. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

The tab is also used 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, 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.

> **NOTE:** When changes to authentication and authorization configurations are made, clients must be restarted in order to be subject to the new configuration. It is suggested that you disconnect those clients affected by the changes made to your authentication and authorization configurations. You can use the Client Connections tab in the Server Information window to help identify which clients are affected by the changes, and disconnect those clients.

This Help topic contains an explanation of the different sections and fields in the User/Group tab. For complete steps in configuring authentication methods and creating authorization groups, see How to Configure User Access to Extreme Management Center Applications.
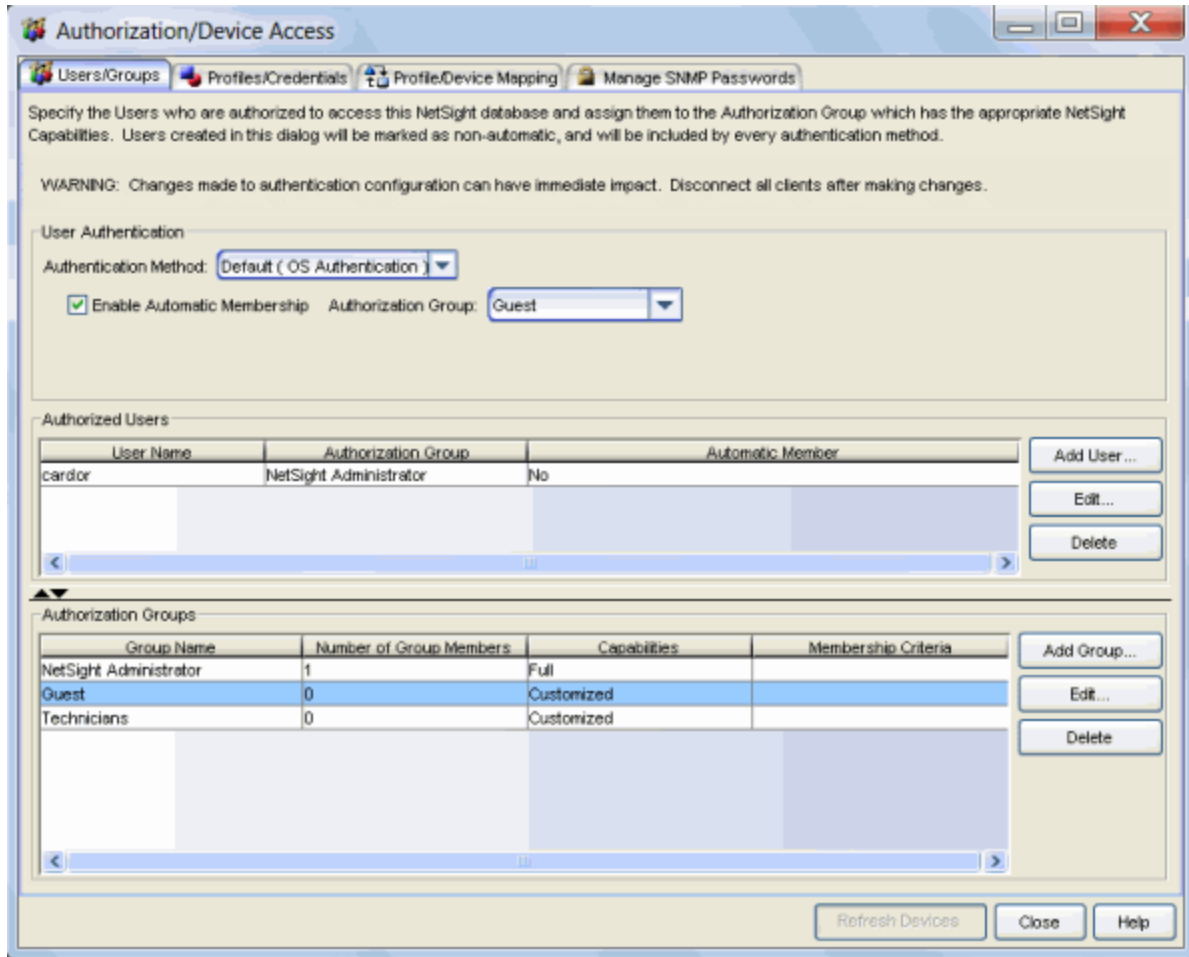
User Authentication

Use this section to configure the method that will be 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 or the NAC Manager Dashboard. The following authentication methods are available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

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 that will be allowed access and define their access capabilities.
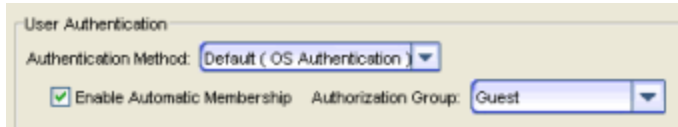
If desired, enable Automatic Membership and specify an authorization group. The Automatic Membership feature allows a user who has not been manually added to the Authorized Users table to be authenticated by the operating system, and dynamically added to the table and assigned to the specified authorization group the first time that they log in. These users are indicated by a "Yes" in the Automatic Member column of the Authorized Users table.

LDAP Authentication

With this authentication method, the Extreme Management Center Server uses the specified LDAP configuration to authenticate users.
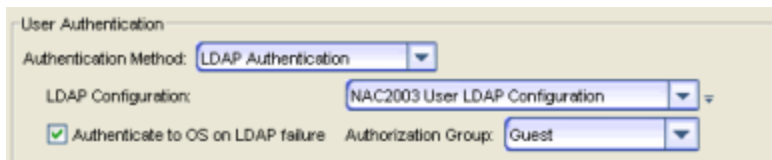
Use the drop-down list to select the LDAP configuration for the LDAP server on your network that you want to use to authenticate users. Use the configuration menu button ⬇ (to the right of the drop-down list) to add or edit an LDAP configuration, or manage your LDAP configurations.

With LDAP Authentication, you can configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, you could 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 that has 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 LDAP failure** feature provides the option to use OS Authentication automatic membership if the LDAP authentication should fail for any reason. 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 "Yes" in the Automatic Member column of the table.

RADIUS Authentication

With this authentication method, the Extreme Management Center Server uses the specified RADIUS servers to authenticate users.

NOTE: The RADIUS Authentication mode supports the PAP authentication type.

Use the drop-down list to select the primary RADIUS server and backup RADIUS server (optional) on your network that you want to use to authenticate users. Use the configuration menu button (to the right of the drop-down list) to add or edit a RADIUS server, or manage your RADIUS servers.

With RADIUS Authentication, you can 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 that has 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 RADIUS failure** feature provides the option to use OS Authentication automatic membership if the RADIUS server authentication should fail for any reason. 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 "Yes" 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. From here you can 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 was added as an Automatic Member.

Users that are manually added to the Authorized Users table using this tab will have the "automatic" attribute in the table set to No. These users have 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 that have been created as authorized users.

Authorization Group
> The authorization group where the user is a member.

Automatic Member
> **Yes** indicates that the user was automatically added to the authorization group via LDAP or RADIUS authentication, or the OS Authentication Automatic Membership feature. **No** indicates that the user is an authorized user that was manually added to the table.

Add User
> Opens the Add User window where you can define the username, domain, and authorization group for a new authorized user.

Edit (User)
> Opens the Edit User window where you can modify the authorization group membership for the selected user.

Delete (User)
> Removes the selected User from the Authorized Users table.

Authorization Groups Table

This table lists all of the authorization groups that have been created. Authorization groups define the access privileges to the Extreme Management Center application features. Based on their membership in a particular authorization group, users are granted specific capabilities in the application.

When users are added to the Authorized Users table, they are assigned an authorization group. With LDAP or RADIUS authentication, users are dynamically assigned to authorization groups based on the attributes associated with that user in Active Directory. The attributes are used to match

against a list of criteria specified as part of each authorization group. The groups are checked in the order they are displayed in this table, from top to bottom. The first group that has a 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 will not be authenticated and will not be allowed to log in. For this reason, it is recommended to 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. This will help differentiate between a user who cannot authenticate successfully, and a user who does not belong to any group.

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. The Extreme Management Center Administrator group cannot be deleted and its capabilities can be viewed, but cannot be changed.

Number of Group Members
> 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).

Membership Criteria
> This column displays the membership criteria defined for the associated group.

Add Group
> Opens the Add Group window where you can define the capabilities and settings for a new group.

Edit (Group)
> Opens the Edit Group window where you can modify the capabilities and settings for a selected group.

Delete (Group)
> Removes the selected group from the Groups table.

Add/Edit User Window

This window lets you define a user's user name, domain, and membership in an authorization group. This information will be used to authenticate the user to the Extreme Management Center (Extreme Management Center) database.
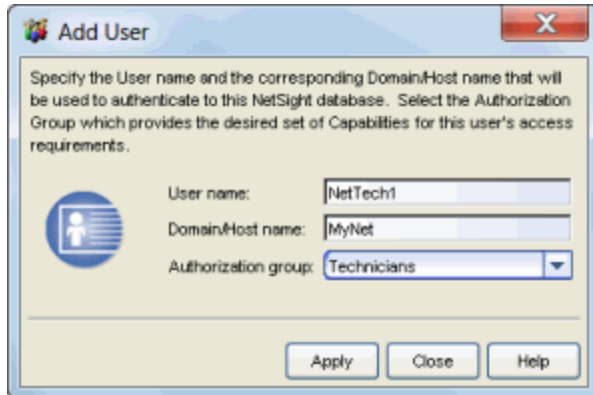
User name
> The name used for this authorized user.

Domain/Host name
> The user's domain/hostname that will be used to authenticate to the Extreme Management Center database.

Authorization Group
> Use the drop-down list to select the authorization group where this user will be a member.

Add/Edit Group Window

This window lets you define a new authorization group or edit an existing group. For a description of each capability, see [Authorization Group Capabilities](#).
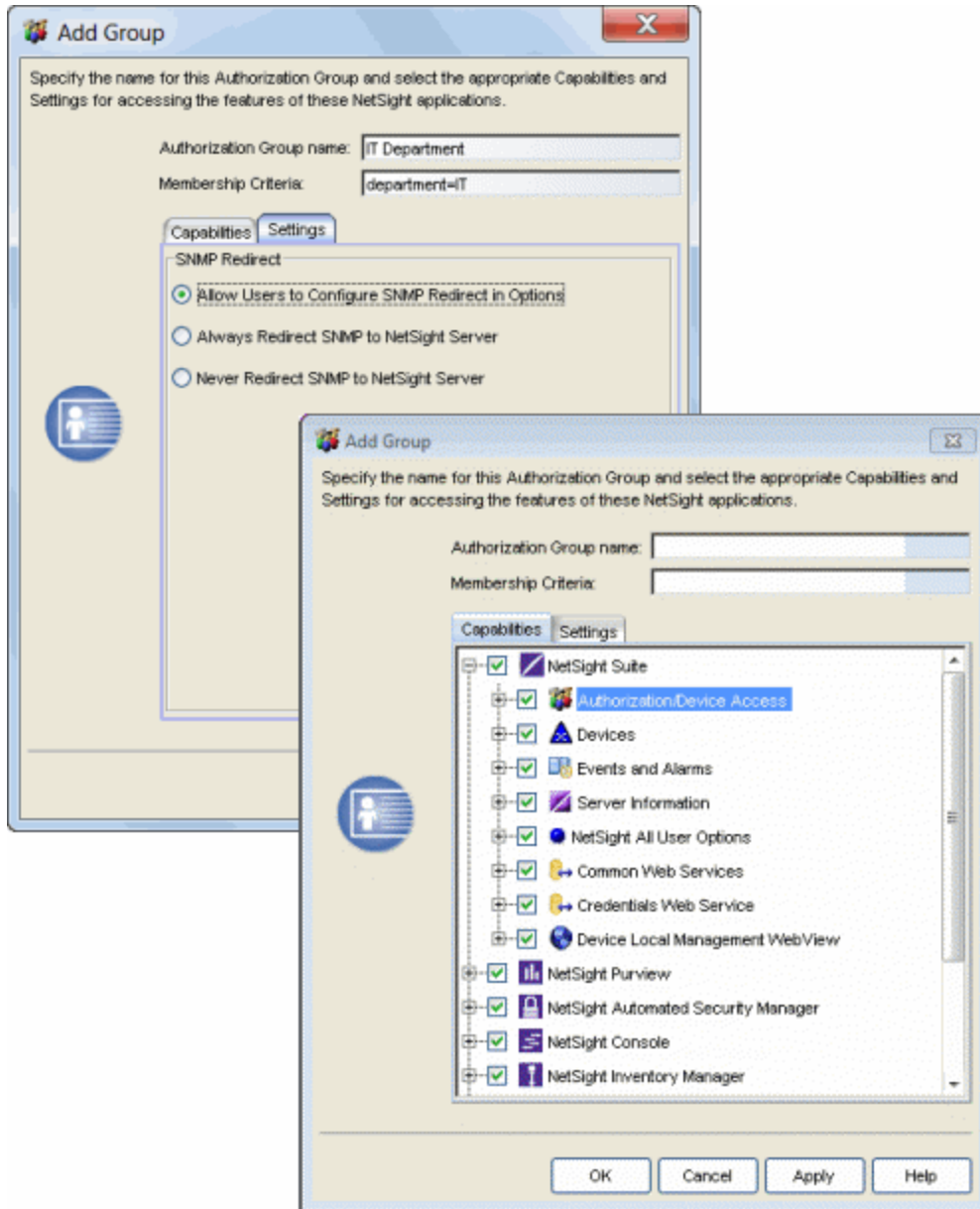
Authorization Group Name

> This is the name given to the group. When adding a group, you can 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: You cannot define membership criteria for the Extreme Management Center Administrator Group. Membership in the administrator group must be assigned manually using the Authorized Users table.

Capabilities Tab

Expand the Capabilities tree in this tab and select the specific capabilities to be granted to users that 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](#).

Settings Tab

The Settings tab configures how SNMP requests will be handled for users that are members of this group.

Allow Users to Configure SNMP Redirect in Options

Lets users edit the Suite-wide Option setting for Client/Server SNMP Redirect.

Always Redirect SNMP to NetSight Server

Redirects all SNMP requests to the Extreme Management Center (NetSight) Server, regardless of the Suite-wide Option setting for Client/Server SNMP Redirect.

Never Redirect SNMP to NetSight Server

Never redirects SNMP requests to the Extreme Management Center (NetSight) Server, regardless of the Suite-wide Option setting for Client/Server SNMP Redirect.

Related Information

For information on related windows:

- [Profiles/Credentials Tab](#)
- [Profile/Device Mapping Tab](#)
- [Manage SNMP Passwords Tab](#)

For information on related tasks:

- [How to Manage SNMP Passwords](#)
- [How to Configure Profiles and Credentials](#)
- [How to Configure Profile/Device Mapping](#)
- [How to Configure User Access to Extreme Management Center Applications](#)

Manage SNMP Passwords Tab (Legacy)

This tab lets you collectively manage the credentials that have been set on your network's devices. When a particular credential is selected from the drop-down menu above the table, the table lists the devices where that credential/password is set. When an SNMPv1 or SNMPv2 credential is selected, you can define a *New Community Name* for access to the devices in the table. When an SNMPv3 credential is selected, you can define both the *Authentication* password and the *Privacy* password for access to the devices in the table. You can assess the impact of applying new passwords on your devices before actually applying them by clicking **Test** and checking the information in the **Test Results** column.

Select Credential

 This drop-down list contains all of the Credentials that have been created in the Extreme Management Center database.

New Community Name

The new (SNMPv1/2) community name that will be used for access to the associated device(s).

Authentication/Privacy

The new SNMPv3 passwords that will be used for access to the associated device(s).

Show Passwords in Clear Text

When checked, the passwords are shown in text. When unchecked, the passwords are shown as a string of asterisks.

Credentials Table

This table lists all of the devices where the selected credential can be used.

Device

The list of devices where the currently selected credential can be used to access the device.

Auth Group

This is the Authorization Group(s) that are granted access to the associated device.

Profile

This is the profile used by the associated Authorization Group for access to the device.

Read, Write, Max Access

These columns show the credential used for each access level.

Use for Set

Shows the credential that is used with the SNMP Set to change the credential on the device.

Test Results

After clicking Test, this column shows the results that can be expected if the credential changes are actually applied to devices.

Results

After clicking **Apply**, this column shows the results of the credential changes that were applied to devices.

Refresh Button

Updates the table when information has changed.

Test Button

This button lets you view the results that can be expected if your credential changes are actually applied to the devices.

Apply Button

Related Information

For information on related windows:

- Users/Groups Tab
- Profile/Device Mapping Tab
- Profiles/Credentials Tab

For information on related tasks:

- How to Manage SNMP Passwords
- How to Configure Profiles and Credentials
- How to Configure Profile/Device Mapping
- How to Manage Users and Groups

Command Script Tool

The Extreme Management Center Command Script tool lets you execute a sequence of CLI commands (a script) on a set of devices. This can be useful for many purposes, such as modifying a number of device configurations at one time. The Command Script tool uses either SSH or Telnet to connect to a device, depending on the connection type configured in the device's CLI credentials. If the connection type is SSH, be sure that SSH access is enabled on the selected device.

Instructions on:

- [Launching the Command Script Tool](#)
- [Creating and Executing a Command Script](#)
    - [Script Variables](#)
    - [Meta Commands](#)
- [Authentication](#)
- [User Capabilities](#)
- [Device Menu Integration](#)
- [Example Command Scripts](#)

Launching the Command Script Tool

The Command Script tool can be launched from the device tree in Extreme Management Center Console or Inventory Manager. You can have multiple Command Script windows open at the same time.

From Console:
Right-click on any number of devices or device groups in the left-panel device tree, and select Execute Command Script from the menu.

From Inventory Manager:
Right-click on a single device or device group in the left-panel device tree, and select Execute Command Script from the menu. You can also select a device or device group and then select Execute Command Script from the Tools menu.

The Command Script Tool window opens with the selected devices displayed in the Devices list in the lower left. Use the Devices toolbar buttons ⬛⬛ to add and delete devices to and from the list, if desired.
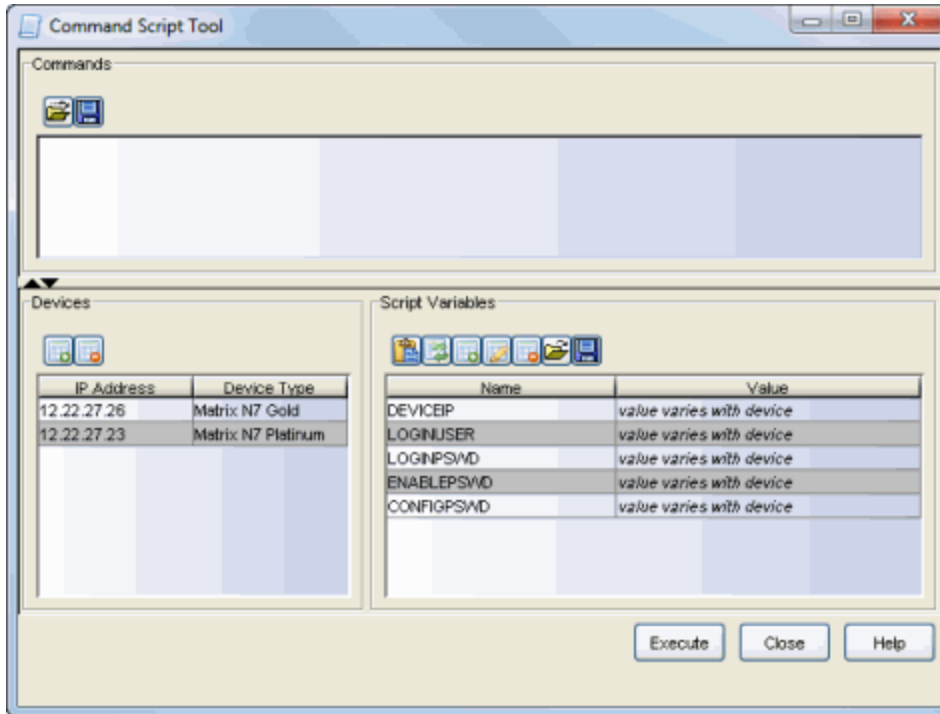
Creating and Executing a Command Script

Once you have launched the Command Script Tool, you can enter a sequence of commands into the Commands text box.
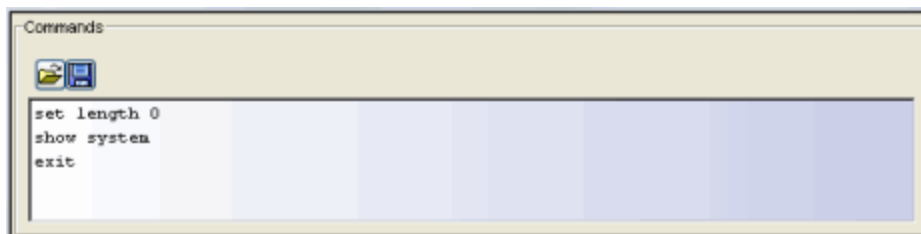
> **Load Script from File** - Lets you load a script from a local file or a file on the Extreme Management Center Server. Scripts on the Extreme Management Center Server must be stored in the <install directory>/appdata/CommandScriptTool/ directory in order to be accessed from this Load Script From File button.

Save Script to File - Once you have created your script, you can save it to a local file.

When creating a command script, it is important to keep the following instructions in mind:

- Begin each script with a command that turns off paged output. Paged output requires that you repeatedly respond to a "more" prompt when a command generates many lines of output. Since the size of the output can vary or may not be known, it is impossible to include responses to "more" prompts in a reliable way. Turning off paged output means that you do not have to include responses to the "more" prompts in your script. The command to turn off paged output varies with different device types. The screenshot above shows a command script for an N-Series device that includes the command "set length 0" to turn off paged output.

- Include commands that persist changes, if necessary. For example, to append or otherwise change a device's configuration, the script will need to include the commands to change mode and the commands to persist the new configuration.

- Make sure the command script cleanly logs out of the device before terminating to properly free device resources. A script that does not cleanly log out might fail to free all resources in the device when the SSH connection is terminated. Repeatedly executing such scripts might eventually tie up resources to the point where SSH connections to the device can no longer be made.

Once the commands are ready, click the **Execute** button to execute the commands on the selected devices. A Results window opens and displays the progress and results of the commands on each device. At the top of the Results window is a table showing the script execution status of each device. The bottom of the window displays the command output for the device selected in the status table above. Use the **Save Results** button to save the results for all the devices to a text file.
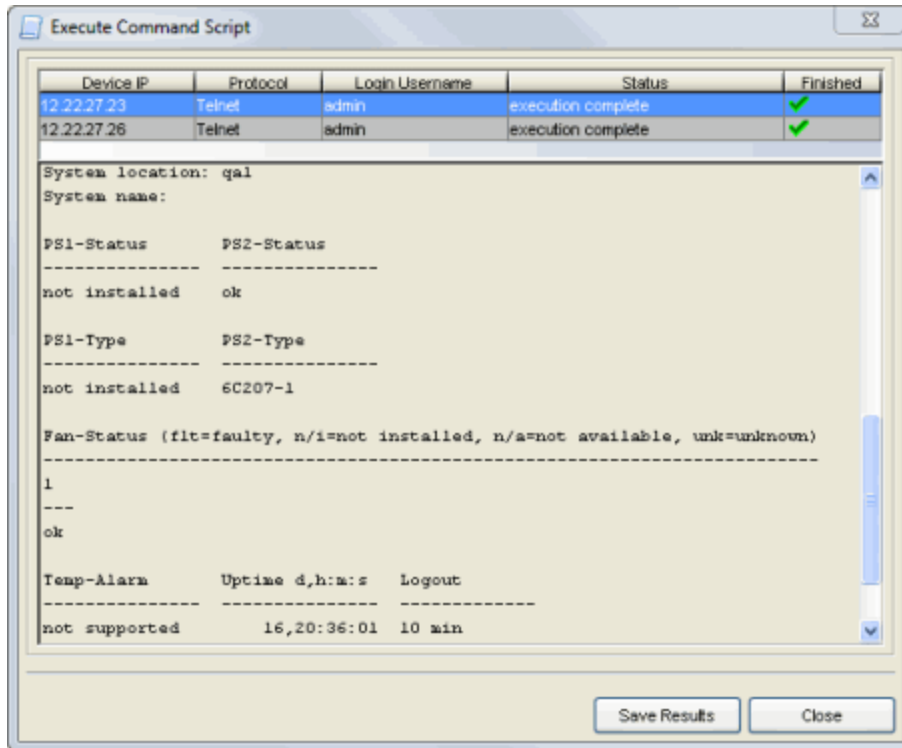
If there are errors connecting to or logging into a device, or if the device returns an error to any command, an error message will be displayed in the output area of the results window.

Script Variables

The Command Script tool supports the use of variables within scripts. The variable must appear in the script bracketed by percentage signs, for example, %TYPE%, as shown in the command script below.
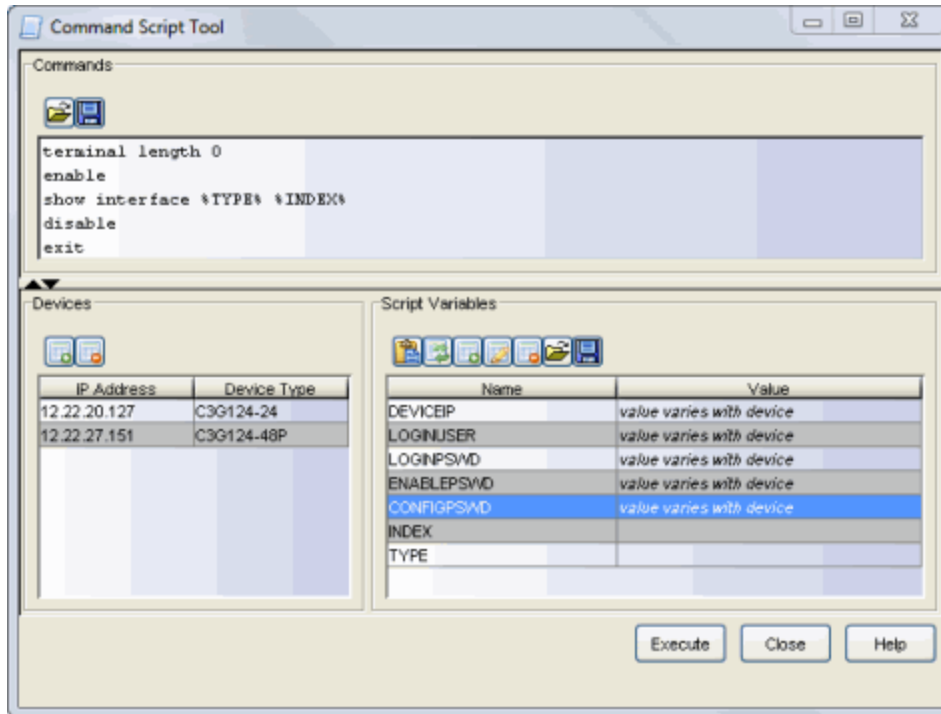
There are two kinds of variables: system variables and user variables. The following table lists the differences between system and user variables:

System Variables	User Variable
System-defined variable names.	User-defined variable names.
System-defined variable values.	User-defined variable values.
Values differ on each device.	Values are the same on each device.

Extreme Management Center provides five system-defined variables:

%DEVICEIP% - The IP address of the currently selected device.

%LOGINUSER% - The login username configured in the Profile of the selected device.

%LOGINPSWD% - The login password configured in the Profile of the selected device.

%ENABLEPSWD% -The enable password configured in the Profile of the selected device.

%CONFIGPSWD% - The config password configured in the Profile for the selected device.

You can create user-defined variables two ways using the toolbar buttons for the Script Variables table in the lower right portion of the Command Script window. You can add a variable to the table using the Add Variable button, and then use the Use Variable button to insert the variable into the script at the cursor. Or, you can manually enter a variable into the script, and then use the Refresh Variables button to add the variable to the variables table.

Use Variable in Script - Inserts the selected variable into the script at the current cursor location.

Refresh Variables from Script - Scans the script for variables, adding new variables and removing unused user variables from the variables list.

Add Variable - Lets you add a user variable to the variables list.

Edit Variable - Lets you modify a user variable value.

Delete Variable - Lets you delete the selected user variable from the variables list.

Load Variables from File - Lets you load in user variables from a local file or a file on the Extreme Management Center Server. Variables on the Extreme Management Center Server must be stored in the <install directory>/appdata/CommandScriptTool/ directory in order to be accessed from this Load Variables from File button.


Save Variables to File - Lets you save the user variables into a local file.

Meta Commands

Meta-Commands are commands that are executed by the Command Script tool, not by the device:

- @KEY [*c* | %xx] - Enters a single character *c*, or a single character ASCII xx (hexadecimal) with no end -of-line characters.

- @SLEEP *n* - Pauses (does nothing) for *n* seconds.

- @RECEIVE *n* - Receives device output for *n* seconds.

- @ENDOFLINE [CR | CRLF | LF] - Specifies the end-of-line characters sent to the device after each command. This meta command affects all subsequent commands.

- @COMMANDDONE *n* - The script will wait for *n* seconds for command output before a command is considered done. This meta command affects all subsequent commands. *n* is an integer between 1 and 86400 seconds.

For example:

`@key m` - equivalent to a user pressing the M key

`@key %20` - equivalent to a user pressing the space bar.

If there are errors processing meta-commands, an error message will be displayed in the output area of the Results window at the point where the command was executed.

Authentication
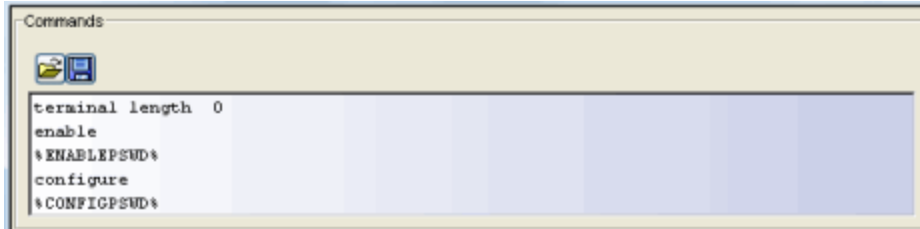
The Extreme Management Center Authorization/Device Access tool (accessed from the application's Tools menu) is used to configure the profiles and credentials that provide access your network devices. Each device is assigned a profile and that profile designates the CLI credentials to use for that device.

CLI credentials include the following information:

- User name

- Login Password

- Enable Password

- Configuration Password

- Connection Type - SSH or Telnet

The Command Script tool uses the connection type (SSH or Telnet), user name, and login password specified in the CLI credentials when establishing a connection to the device. If these are not set up correctly, the connection cannot be created. You can view the user name and connection type (protocol) that was used by the Command Script tool in the Results window.

CLI credentials are also available as system-defined variables that can be used in scripts. These variables are useful to satisfy prompts that may occur while the script is executing, as shown below.

User Capabilities

You must be assigned the appropriate user capability to execute command scripts. Capabilities are assigned via a user's authorization group, which is configured using the Authorization/Device Access tool. The capability is NetSight (Extreme Management Center) Suite > Devices > Execute Command Scripts.
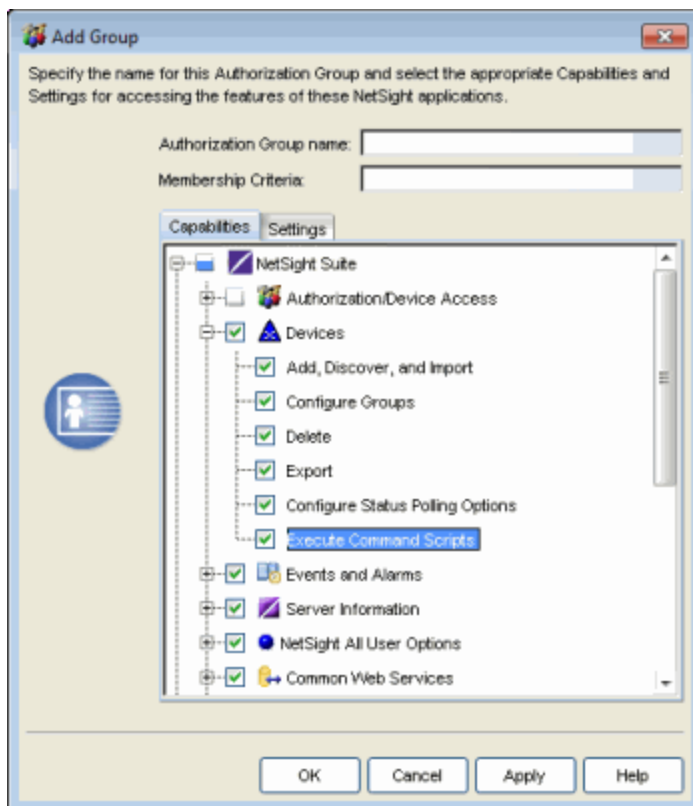
Device Menu Integration

You can add a command script as a menu item to the device right-click menu by creating a menu definition in the ThirdPartyMenu.xml configuration file located in the NetSight\appData\System\Shared directory. Instructions for creating these definitions can be found in that file. You must restart the Extreme Management Center Server before the modified version of this file will be deployed to connecting clients.

In the configuration file, command script menu items are defined with a <menu> element that contains a <commandscript> element. A <commandscript> element can only be used with a <menu> element with type="device-menu" as shown below.

```
<menu id="version" name="Show Version"
      icon="script.png"type="device-menu">
    <commandscript name="Show Version">
        <command>show version</command>
        <command>exit</command>
    </commandscript>
</menu>
```

The <commandscript> element defines a command script and assigns it a name. The <command> elements contained within the <commandscript> element provide each line of the script. Note that because the commands are contained in an XML document, special characters such as "<", ">", and "&" need to be escaped as entity references: <, >, and &, respectively.

The menu item will appear in the right-click popup menu in the Console device tree, but only if a single device is selected. If that menu item is selected, the command script will be executed immediately on the selected device.

A command script provided in the third-party menu definitions can use both system-defined and user variables. If user variables are included in the command script (as shown below), you will be prompted for values before the command executes.

```
<menu id="version" name="Show Interface"
icon="script.png" type="device-menu">
    <commandscript name="Show Interface">
        <command>show interface %IFNAME%</command>
        <command>exit</command>
```

```
        </commandscript>
    </menu>
```

You can configure command script menu items to be displayed only for certain devices by having the <commandscript> element include qualifying elements that identify those device types. The two qualifying elements are <devicetype> and <sysoid>, as shown below. If no qualifying elements are used, the menu item will appear on all devices.

```
    <menu id="config" name="Show Configuration"
    icon="script.png" type="device-menu">
        <commandscript name="N-Series Show Configuration">
     <devicetype pattern="Matrix N\d.*"/>
            <command>set length 0</command>
            <command>show running -config</command>
            <command>exit</command>
        </commandscript>
        <commandscript name="XSR Show Configuration">
     <sysoid prefix="1.3.6.1.4.1.5624.2.1.32">
     <sysoid prefix="1.3.6.1.4.1.5624.2.1.45">
            <command>terminal length 0</command>
            <command>enable</command>
            <command>show running -config</command>
            <command>disable</command>
            <command>exit</command>
        </commandscript>
    </menu>
```

A <devicetype> element matches devices by using a regex pattern to match a device's displayed device type. For example, <devicetype pattern="Matrix N\d.*"/> will match any Matrix N1 Platinum device, any Matrix N3 Platinum device, and so on.

A <sysoid> element matches devices by a full or partial match on the device's system object identifier. For example, <sysoid prefix="1.3.6.1.4.1.5624.2.1.45"/> will match any XSR-1850.

If there are several qualifying elements within a <commandscript> element, the menu item will be displayed on any device that matches any qualifying element.

 Additionally, multiple <commandscript> elements can be configured for the same menu item. When the menu item is selected, the command script that

matches the device will be launched. In this way, one menu item can be configured to launch different scripts for different devices.

Example Command Scripts

Following are examples of different ways to use command scripts:

To collect data from a range of devices:

```
set length 0
show igmp counters
exit
```

To make duplicate modifications to a range of devices:

```
set banner motd
In case of problems, contact Joe Smith x1234
END
```

To modify and save the running configuration on a device:

```
router
config
set vlan create 3
set vlan name 3 green
write file
exit
exit
exit
```

To display system settings:

```
set length 0
show system
```

To enable SNMPv2 according to existing SNMPv1 settings on all devices:

```
set snmp group NetOpRO user ebinu security-model v2c
set snmp access NetOpRO security-model v2c privacy
exact read All
notify All
set snmp group NetOpRW user fbnet1991 security-model
v2c
set snmp access NetOpRW security-model v2c privacy
```

```
exact read All
notify All
```

To roll out SNMPv3 on all N-Series, Stackable, and Standalone devices:

```
set snmp user netopro auth md5 ebinu#netro priv
D1PwfdVvSbR0
set snmp user netoprw auth md5 ebinu#netrw priv
D2PwfdVvSbRW
set snmp group NetOpRO user netopro security-model usm
set snmp group NetOpRW user netoprw security-model usm
set snmp access NetOpRO security-model usm privacy
exact read All
notify All
set snmp access NetOpRW security-model usm privacy
exact read All write All
notify All
```

To configure SNTP on all N-Series, Stackable, and Standalone devices of a specific area:

```
#sntp
set sntp client unicast
set sntp server 130.92.9.51
# timezone
set timezone CET 2 0
```

Related Information

- [How to Configure Profile/Device Mapping](#)

- [How to Configure Profiles and Credentials](#)

- [How to Manage Users and Groups](#)

ExtremeNetworks.com Product and Firmware Updates Via Extreme Management Center

Extreme Management Center applications provide an easy way to access the Extreme Networks website to obtain information about the latest Extreme Management Center product releases and Extreme Networks firmware releases available for download.

How to Check for Updates

Extreme Management Center applications provide an easy way to access the Extreme Networks website to obtain information about the latest Extreme Management Center product releases and Extreme Networks firmware releases available for download.

Instructions on:

- Checking for Extreme Management Center Updates

    - Scheduling a Check for Updates

- Checking for Firmware Updates

Checking for Extreme Management Center Updates

Use the following steps to check for Extreme Management Center software updates available for download. If updates are available, you can download the updates from the Extreme Networks website. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to perform the check for updates.

Before using the Check for Updates feature, it is important to configure your Update Credentials in the ExtremeNetworks.com Update Suite options (**Tools > Options**). 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 Extreme Management Center updates:

1. From any Extreme Management Center application, select **Help** > **Check for Updates** in the menu bar.

2. The Updates Available window opens where you can view the new updates that are available for download.

3. Click on the **Download Release** link to access the website and navigate to the Network Management Suite (NMS) software download page where you can initiate the download. Click on the **Release Notes** link to open a PDF of the Extreme Management Center release notes. You need to enter credentials to access the website; use the same credentials configured in the ExtremeNetworks.com Update Suite options (**Tools > Options**).

Scheduling a Check for Updates

You can schedule a routine check for Extreme Management Center updates that takes place automatically.

1. Select **Tools > Options** in the menu bar. The Options window opens.

2. In the left-panel tree under Suite options, select ExtremeNetworks.com Update.

3. In the right-panel Schedule Updates section, select the desired schedule: **Daily** or **Weekly**.

4. If you have specified a **Weekly** check, use the drop-down menu to select the day of the week you wish the check to be performed, and set the desired time. If you have specified a **Daily** update, set the desired time.

5. If your network is protected by a firewall, click the **Edit** button in the HTTP Proxy Server section 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. Click **OK** to close the window.

6. In the Update Credentials section, enter the credentials used to access the ExtremeNetworks.com website to obtain update information.

7. Click **OK** to set the options and close the window.

8. When the scheduled update check is performed, a message in the Event Log informs you if updates are available.

9. If updates are available, select **Help > Check for Updates** in the menu bar.

10. The Updates Available window opens where you can view the new updates available for download. Click on the **Download Release** link to access the website and navigate to the Network Management Suite (NMS) software download page where you can initiate the download. Click on the **Release Notes** link to open a PDF of the Extreme Management Center release notes.

> **TIP:** The last time Check for Updates executed successfully is reported in the Help > About Extreme Management Center window.

Checking for Firmware Updates

Use the following steps in Inventory Manager to check for firmware updates available for the devices in the Extreme Management Center database. If updates are available, you can download the updates from the Extreme Networks website. Once you have downloaded the updates, you can use the Firmware Upgrade Wizard to upgrade your network devices. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to perform the check for updates.

Before using the Check for Updates feature, it is important to configure your Update Credentials in the ExtremeNetworks.com Update Suite options (**Tools > Options**). 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. In Inventory Manager, select **Tools > Check for Firmware Updates** in the menu bar.

2. The Updates Available window opens where you can view the new updates that are available for download.

3. Click on the **Download Release** link to access the website and navigate to the product Firmware download page where you can initiate the download. Enter credentials to access the website; use the same credentials configured in the ExtremeNetworks.com Update Suite options (**Tools > Options**).

Related Information

For information on related windows:

- [Updates Available Window](#)

Updates Available Window

Extreme Management Center applications provide an easy way to access the Extreme Networks website to obtain update information about the latest Extreme Management Center product releases and firmware releases available for download. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to perform the update function.

For complete instructions, see [How to Check for Updates](#).

Check for Extreme Management Center Updates

To check for Extreme Management Center software updates that are available for download, select **Help > Check for Updates** in the menu bar in any Extreme Management Center application. The Updates Available window displays any updates that are available and let you initiate the download operation.

Click on the Download Release link to access the Extreme Networks website and navigate to the Network Management Suite (NMS) software download page where you can initiate the download. Click on the Release Note link to open a PDF of the Extreme Management Center release notes for the new version. You need to enter credentials to access the website; use the same credentials that are configured in the ExtremeNetworks.com Update Suite options (**Tools > Options**).

Check for Firmware Updates

To check for firmware updates that are available for download, select **Tools > Check for Firmware Updates** from the Inventory Manager menu bar. The Updates Available window displays any firmware updates that are available for the devices in the Extreme Management Center database, and let you initiate the download operation.

Click on the **Download Release** link to access the Extreme Networks website and navigate to the product Firmware download page where you can initiate the download. You need to enter credentials to access the website; use the same credentials configured in the ExtremeNetworks.com Update Suite options (**Tools > Options**).

Related Information

For information on related tasks:

- How to Check for Updates

Event View

The Extreme Management Center Event View (located at the bottom of the legacy Console java application main window) lets you view alarm, event, and trap information for Console and other Extreme Management Center applications. In addition, the Extreme Management Center Event View provides access to the Event Log Viewer which lets you view historic alarm, event, and trap information. It also provides access to the Event View Manager window where you can add your own tabs to the event view panel to create custom tables that provide the information needed to manage your network.

The Extreme Management Center Event View is used only in the Console application and the information in the Help topics in this folder applies to the Extreme Management Center Event View only. The other Extreme Management Center applications have different event views, and Help topics on those event views are available in the online help for the specific application.

Event View

Extreme Management Center's Event View lets you view alarm, event, and trap information for Extreme Management Center Console, network devices, and other Extreme Management Center applications. Each tabbed view in the Event panel lets you scroll through the most recent 10,000 entries in the logs that are configured for that view.

When Extreme Management Center Console is initially installed, the following tabs are provided: a **Console** tab showing Console events, an **Alarms** tab showing network alarms, and a **Traps** tab that captures traps from devices modeled in the Extreme Management Center database. The **Syslog** tab shows events from devices that are configured to use the Extreme Management Center Syslog Server.
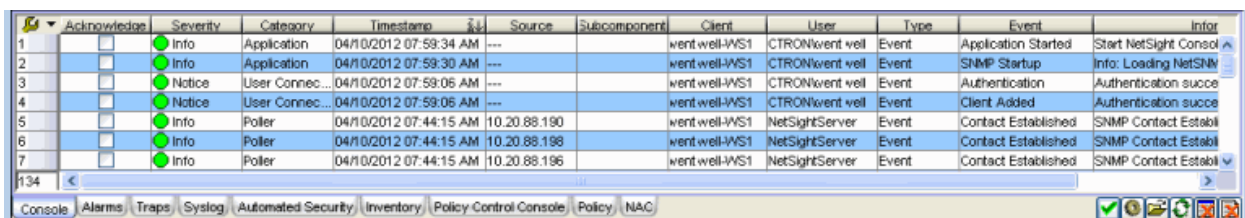
In addition, there is a tab for each installed Extreme Management Center application, as well as a **Scheduler** tab that displays events for the Extreme Management Center scheduled tasks configured via the **Administration** tab.

You can add your own tabs that capture local logs. Local logs are not automatically polled, but can be manually refreshed using the **Refresh** button.

With the Event tables, you can:

- Configure your own tables to capture and combine similar information from various sources. For example, you can combine event logs from other Extreme Management Center applications or merge trap logs into an single Event View.
- Find, filter, and sort table information.
- Print table information
- Use the auto-export toolbar to export Event View information to a file in HTML or delimited text format.
- Trigger e-mail notification, when a particular alarm, event, or trap occurs.

Sample Event View

Tabs

Depending on your installation, up to four default tabs are available with the initial installation of the legacy Console java application. You cannot remove or change these tabs. However, you can add your own tabs to create custom tables that provide the information needed to manage your network.

The four default tables are:

Console Tab
> This tab records Console events, such as devices created or deleted, discovery started or ended, and poll activity.
>
>> **TIP:** You can also view the Console Event Log via a web browser using the Extreme Management Center **Alarms and Events** tab.

Alarms Tab
> This tab shows information about current network alarms. You can also clear alarms and view an alarm history about all current and past alarms.
>
>> **TIP:** You can also view the Alarms tab via a web browser using the Extreme Management Center **Alarms and Events** tab.

Traps Tab
> Shows trap information for devices modeled in the Extreme Management Center database.
>
>> **NOTE:** If no trap information is being collected in the Traps tab, you may have more than one trap daemon running on your system. Console includes an SNMP trap daemon that must be the only trap daemon running on your system. If there is another trap daemon running, either the OS trap daemon or with another application (HPOV, Extreme Management Center Element Manager, etc.), you must shut it down before launching Console.

Syslog Tab
> This tab maintains a record of all the BOOTP messages received for devices modeled in the Extreme Management Center database.

Event Log Column Definitions

Acknowledge

This column can be checked which lets you hide items that have been acknowledged. Click the check box to acknowledge the item and then click the Show Acknowledged Events button to hide or show the checked items.

Severity

Indicates the potential impact of the event or trap. For traps, this column shows the Severity as defined in the `trapd.conf` file.

Category

For traps, this column shows the cagtegory defined in the `trapd.conf` file. For other events, it indicates the source of the of the information, either a Console Poller, local log, syslog, trap log, Error (java exceptions), etc.

Timestamp

Shows the date and time when an event, or trap occurred.

Source

Shows the IP address of the host that was the source of the event, or trap.

Client

Is only applicable to Console events and shows the hostname of the source of the event.

User

Associates an event with 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 event as defined in the `trapd.conf` file.

Information

Shows an summary explanation of the event, or trap.

Right-Click Menu

A right-mouse click on a column heading or anywhere in the table body (or a left-mouse click on the Table Tools 🔧 button when visible in the upper left corner of the table) opens a popup menu that provides access to event options and a set of Table Tools that can be used to manage information in the table. The

right-click menu for the Event View provides the following options in addition to those available as standard options:

- **Acknowledge Selected** - places a check in the Acknowledge column for all of the selected rows.
- **Unacknowledge Selected** - removes the checks in the Acknowledge column from all of the selected rows.
- **Acknowledge All** - places a check in the Acknowledge column for all rows.
- **Unacknowledge All** - removes the checks in the Acknowledge column from all rows.

- **Event Details** - opens the Event Details window which provides additional information about a selected event or trap.

Show/Hide Acknowledged Events

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

Event View Manager

This button opens the Event View Manager window where you can change the elements in the selected table or define additional tabs for the Event View panel.

Open Event Log

This button lets you open an event log file located on the Extreme Management Center Server or Client. The popup menu offers two options:

- **Open Local Event Log** - opens the Open Log file browser with the default path set to the `<install directory>\clients` directory.
- **Open Event Log on Server** - opens the Open Log file browser with the default path set to the `<install directory>\appdata\logs` directory.

Refresh Button

This button forces a poll to update the selected table in the Event View panel.

Clear Current View Button

Clears entries from the current table.

Clear Cache and Roll Logs on Server Button

Writes the current table entries to a timestamped file and clears entries from the table and the server cache. This button acts only on the currently selected tab in the Event panel. Console log files are saved to the

`<install directory>\appdata\logs` directory. Syslog and Traps log files are saved to the syslogs and traps directories respectively, in the `<install directory>\appdata\logs` directory.

Related Information

For information on related windows:

- [Event View Manager Window](#)

For information on related tasks:

- [How to Configure Events](#)

Event Details Window

The Event Details window shows additional information about an event or trap selected in the Event View. To access the window, right-click an event in the Event View and select **Event Details** from the menu. You can also access the window by double-clicking an event.

Timestamp

  Shows the date and time when an event, or trap occurred.

Acknowledged

  Shows whether or not the selected event has been acknowledged.

Type

  Identifies the type of information for this row (Event, or Trap).

Source

Shows the IP address of the host that was the source of the event or trap.

Event Name

Shows the type of event or trap.

Client

The name of the client host machine that triggered the event.

Severity

Indicates the potential impact of the event or trap.

Category

For traps, this field shows the category defined in the `trapd.conf` file. For other tabs, it indicates the source of the of the information, for example, a Console Poller, local log, syslog, trap log, Error (java exceptions), etc.

User

The name of the user that triggered the event.

Information

Shows a summary explanation of the event or trap.

Enterprise

Only applicable to traps and shows the Enterprise for this event (Extreme, Enterasys, snmpTraps, rmonEventsV2, dot1dBridge).

Trap Number

Only applicable to traps and shows the Event OID for this event.

Description

Only applicable to traps and shows the description for this event.

Acknowledge/Unacknowledge

Places a check or removes a check in the Acknowledge column for the selected row.

Related Information

For information on related windows:

- [Event Manager Window](#)
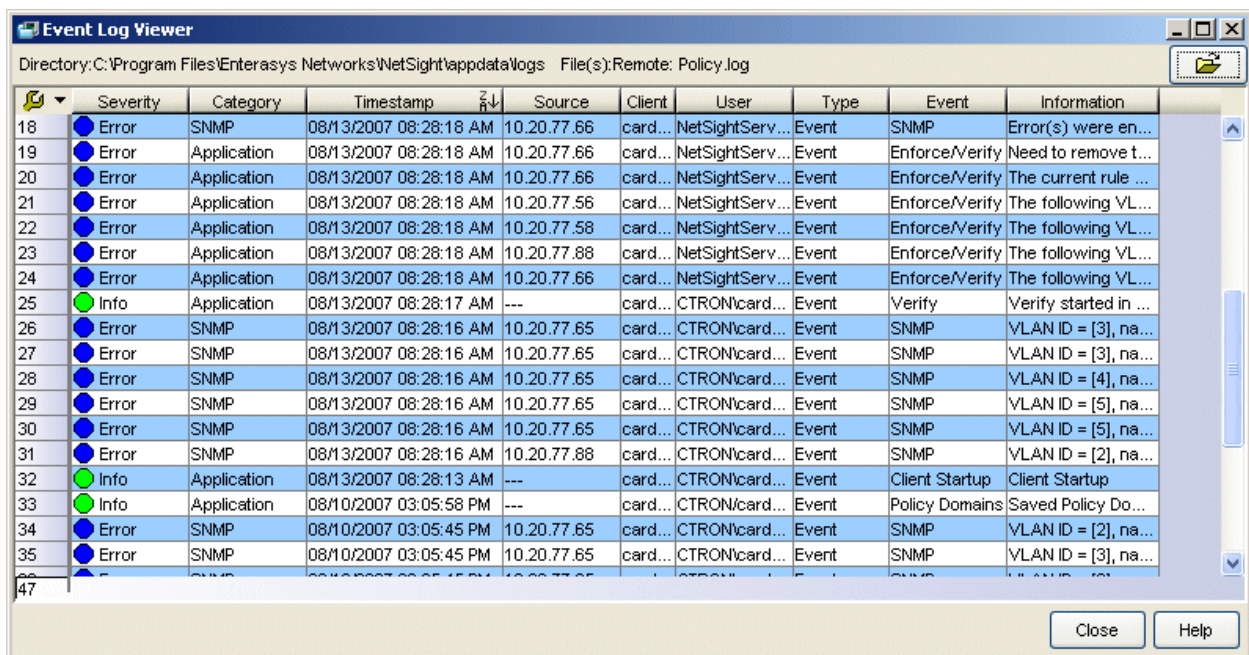
For information on related tasks:

- [How to Configure Events](#)

Event Log Viewer

Using the Extreme Management Center Event Log options, you can set limits on the size of log files that record events on your network. When the limit is reached, the information is saved to a log file. This viewer is where you can view historic alarm, event, and trap information for the legacy Console java application, network devices, and other Extreme Management Center applications. Use the Open Log File window to select a log file to view by clicking the button ![open] in the lower-right corner of the Event View.

Sample Event Log Viewer

Severity

> Indicates the potential impact of the event or trap. For traps, this column shows the Severity as defined in the `trapd.conf` file.

Category

> For traps, this column shows the category defined in the `trapd.conf` file. For other events, it indicates the source of the information, either a Console Poller, local log, syslog, trap log, Error (java exceptions), etc.

Timestamp

> Shows the date and time when an event or trap occurred.

Source

> Shows the IP address of the host that was the source of the event or trap.

Client

> Is only applicable to Console events and shows 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 event as defined in the `trapd.conf` file.

Information

> Shows an summary explanation of the event or trap.

Right-Click Menu

A right-mouse click on a column heading or anywhere in the table body (or a left-mouse click on the Table Tools button when visible in the upper left corner of the table) opens a popup menu that provides access to event options and a set of [Table Tools](#) that can be used to manage information in the table. The right-click menu for the Events Log Viewer provides the following options in addition to those available as standard options:

- **Acknowledge Selected** - places a check in the Acknowledge column for all of the selected rows.
- **Unacknowledge Selected** - removes the checks in the Acknowledge column from all of the selected rows.
- **Acknowledge All** - places a check in the Acknowledge column for all rows.
- **Unacknowledge All** - removes the checks in the Acknowledge column from all rows.

- **Event Details** - opens the [Event Details](#) window which provides additional information about a selected event or trap.

Open Event Log

This button lets you open an event log located in the Extreme Management Center server or client. The popup menu offers two options:

- **Open Local Event Log** - opens the [Open Log File](#) window with the default path set to the `<install directory>\clients` directory.

- **Open Event Log on Server** - opens the [Open Log File](#) window with the default path set to the `<install directory>\appdata\logs` directory.

Related Information

For information on related windows:

- [Event View](#)
- [Event View Manager Window](#)

For information on related tasks:

- [How to Configure Events](#)

Event View Manager Window

The Event View Manager window lets you add your own tabs to the Event View panel to create custom tables that provide the information needed to manage your network. With it, you can add tables and modify existing tables to capture and combine alarm, event and/or trap information from various sources. The top panel lists the current tabs, while the bottom two panels let you define sources for the information in your custom tables.

To access this window, click the Event View Manager button ![icon] in the lower-right corner of the Event View. (If you are using Console, you can also go to the **Tools** menu and select **Alarm/Event > Event View Manager**.)
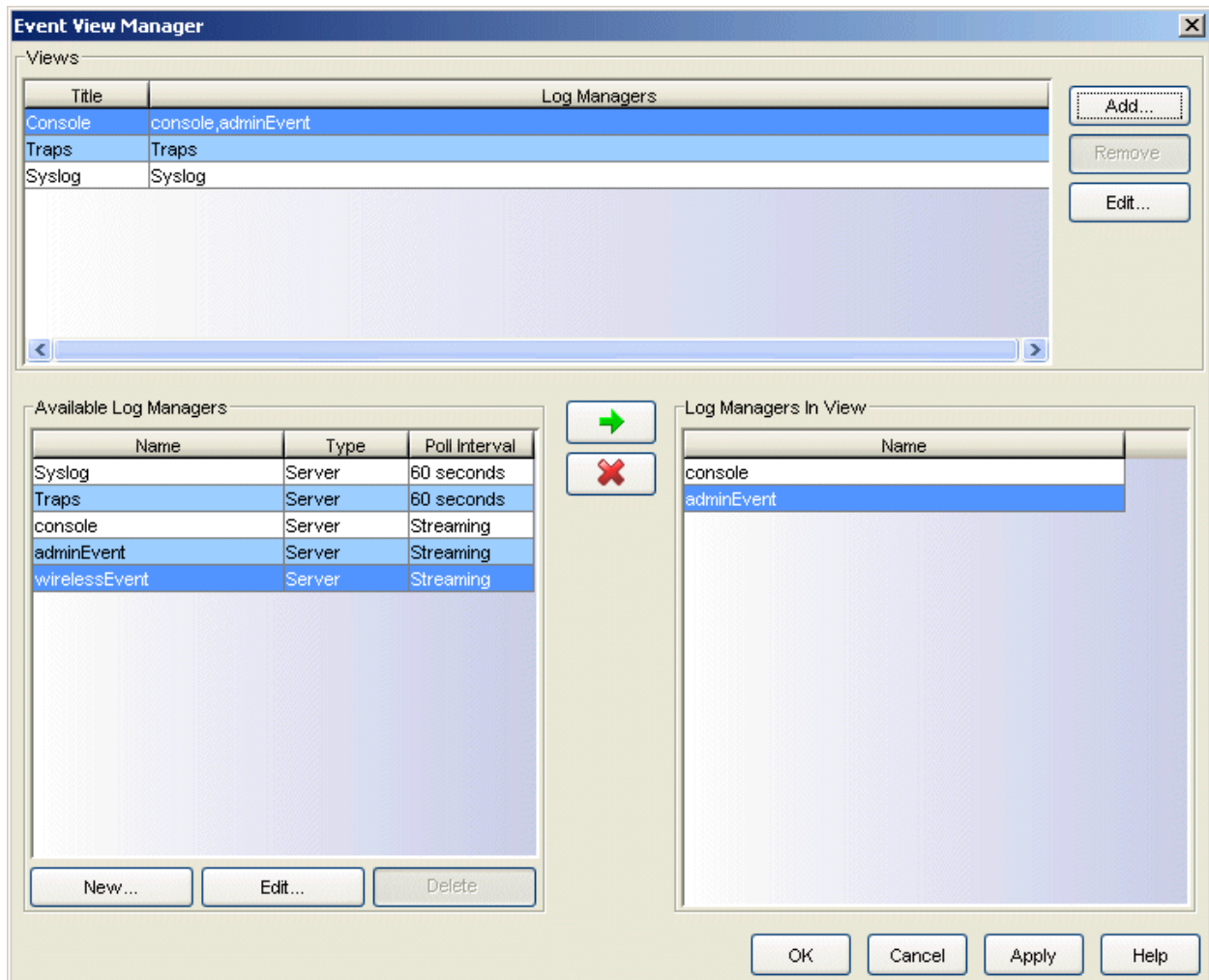
Views

This table lists the currently defined views (tabs) for the Event panel in the main window. Each view can consolidate entries from one or more Log Managers.

- **Title** - The name that appears on the tab in the Event panel.
- **Log Managers** - A comma-separated list of the Log Managers that contribute entries to the view.

Available Log Managers

- **Name** - This is the name assigned to the Log Manager.
- **Type** - Defines the source of the log information: Server or Local.
- **Poll Interval** - Streaming logs are constantly updated. Polled logs are updated at the specified interval. Local Log Managers are Not Polled and must be manually refreshed in the Event panel.

Logs Managers in View

This is a list of the log managers that have been configured for the currently selected view. When you select multiple logs, the information that they provide is merged chronologically in the resulting table in Event tab.

Add Button

This button opens the New View window where you can define the settings for a new Event View and add it to the Views table.

Edit (Event View) Button

This button is active when a View is selected in the Views table. It opens the Edit View window where you can modify the settings for an Event View.

Remove Button

This button deletes the selected Event View from the Views table. The Console, Traps, or Syslog Event Views cannot be removed.

This button adds a Log Manager selected from the Available Log Managers table to the list in the Log Managers in View panel.

This button deletes a Log Manager selected from the list in the Log Managers in View panel.

New Button

This button opens the New Log Manager window where you can define parameters for a new log manager.

Edit (Log Manager) Button

This button opens the Log Manager Parameters window where you can modify parameters for an existing log manager.

Delete Button

This button removes a log manager selected from the Available Log Files.

Apply Button

This button applies the current Event Configurations, but leaves the Event View Manager window open to allow additional configuration.

Related Information

For information on related tasks:

- How to Configure Events

Log Manager Parameters Window

This window displays parameters for a selected log manager. It is opened from the **Edit** button when a log manager is selected in the Available Log Managers area in the Event View Manager window. The window looks different depending on the type of log manager you have selected: server or local.

Use this window to configure the Poll Interval for the Traps Log Manager and the Syslog Log Manager, and to configure the Pattern that will be used to interpret (parse) syslog information managed by the Syslog Manager. You can also use this window to edit parameters for local log managers you have created.
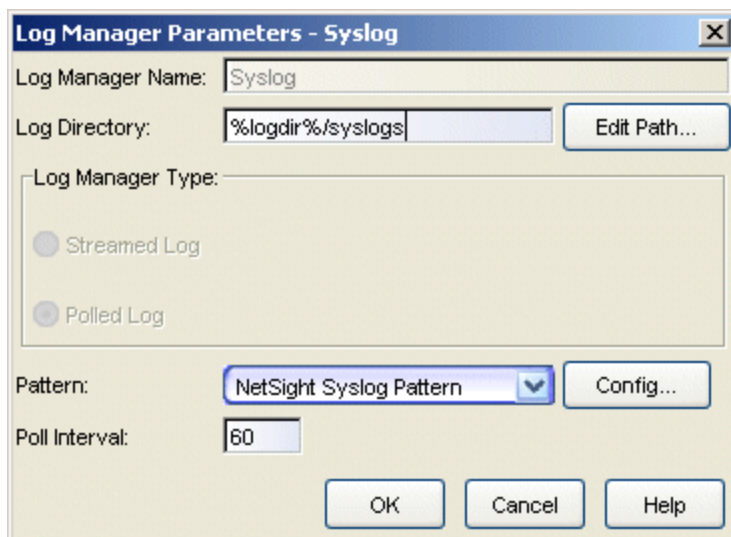
Log Manager Name
  Use this field to edit a local log manager name, if desired.

Log Directory/Log File
  For the Syslog Log Manager, use the Edit Path button to edit the path to the requested syslog file. The path must be a full path residing on the server. For a local log manager you have created, you can edit the path and name or click **Browse** to open a file browser that you can use to select the appropriate log.

Pattern
  This drop-down list is only active when the Syslog Log Manager or a local log manager is selected. You can select a currently defined pattern or click the **Config** button to open the Custom Pattern Configuration window where you can create a

new pattern to match a format that is not parsed by one of the default pattern definitions.

Poll Interval

This field is only active when the Syslog or Traps Log Manager is selected. This is the time interval (in seconds) between retrieving information from the log.

Edit Path Button

Opens the Edit Log Path window where you can edit the path to the requested syslog file. The path must be a full path residing on the server. This button is only available when the Syslog Log Manager is selected.

Config Button

Opens the Custom Pattern Configuration window where you can create a pattern that will be used to interpret information from a non-standard syslog file. This button is only available when the Syslog Log Manager or a local log manager is selected.

Related Information

For information on related windows:

- Events View
- Event View Manager Window

For information on related tasks:

- How to Configure Events

New/Edit (Event) View Window

This window lets you define the name and any columns that you want to add to a new or existing Event View. It is opened from either the **Add** or **Edit** button in the Views area in the [Event View Manager](#) window.
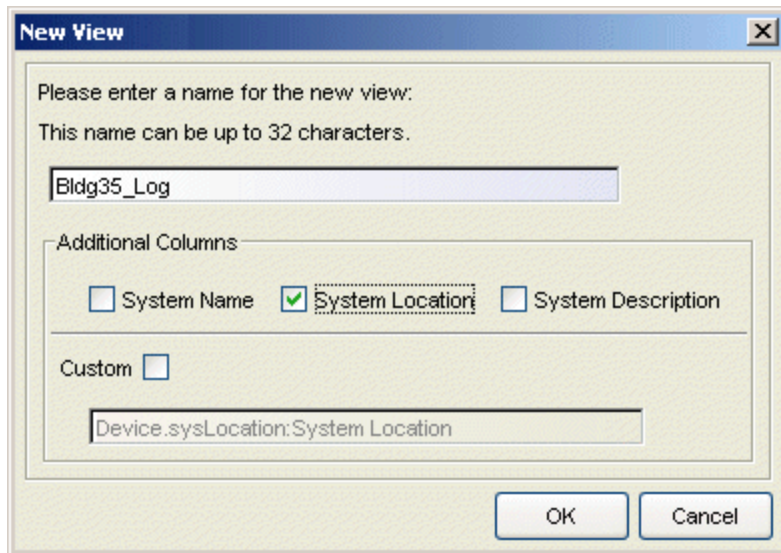
Name

The name for the Event View. This is the name that appears on the tab for this view in the Event View panel.

Additional Columns

You can choose one or more of the three standard column choices (**System Name**, **System Location**, **System Description**) or define your own **Custom** columns. Custom columns can be added for any column from the **NSDEVICES** table. The NSDEVICES table can be found in the **NsSchema.xml** file which is located in the `<install directory>\jboss\server\default\ deploy\NetSight\common\nscoreapi.jar` jar file. Within the jar file, the path is `com\enterasys\netsight\api\Resources\NsSchema.xml`.

One or more columns can be defined as a comma delimited string using the following format:

objName.objField:columnName

where:

objName.objField is the field name from the NSDEVICES table.
columnName is the name that will appear as the column heading.

For example:

chassisID:Chassis

NOTE: Device data in the Event View is not dynamically updated as the device's data changes. You
will need to Refresh the Event View in order to see any changes.

Related Information

For information on related windows:

- Event View Manager Window

For information on related tasks:

- How to Configure Events

New Log Manager Window

The New Log Manager window lets you create local log managers to use when configuring Event Views. It is opened from the **New** button in the Available Log Managers area in the [Event View Manager](#) window.
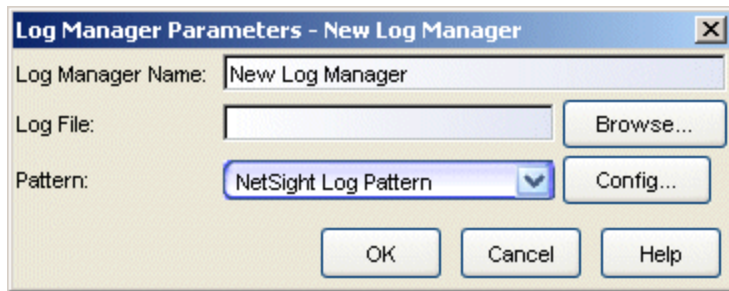
Log Manager Name:
> The name of this log manager.

Log File:
> The path and filename of the log being managed by this log manager. You can type the path and name or click **Browse** to open a file browser that you can use to select the appropriate log.

Pattern
> If you are selecting a syslog file, select a **Pattern** from the drop-down list to be used to interpret the information from the log file. You can select a currently defined pattern or click the **Config** button to open the [Custom Pattern Configuration](#) window where you can create a new pattern to match a format that is not parsed by one of the default pattern definitions:
>
> - **KIWI Pattern** - Parses a basic KIWI Syslog Server file format
> - **NetSight Syslog Pattern** - Parses files generated by the NetSight (Extreme Management Center) Syslog Service
> - **NetSight Trap Log Pattern** - Parses files generated by the snmpTrapd Service
> - **UNIX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service
> - **Console 1.x Pattern** - Parses files generated by Console 1.x
> - **NetSight Log Pattern** - Parses files generated by Console and the other Extreme Management Center applications

- **1X Plugin Pattern** - Parses files generated by the other Extreme Management Center applications
- **Red Hat LINUX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service
- **Ubuntu LINUX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

Config Button

Opens the Custom Pattern Configuration window where you can create a pattern that will be used to interpret information from a non-standard syslog file.

Related Information

For information on related windows:

- Event View Manager Window

For information on related tasks:

- How to Configure Events

Custom Pattern Configuration Window

This window lets you create a pattern used to interpret information from a non-standard syslog file. A sample line is shown un-parsed in the **Sample Log Line**. The **Pattern** line contains **Fields** and **Delimiters** that determine how each data element in the sample line is parsed and placed in a column in the Event View. The **Parsed** table shows how the results presented in the Event View panel.

You can access this window from the **Config** button in the Log Manager Parameters window or the Log Manager Parameters - New window.

Name

This is the Pattern name. You can select one of the standard patterns or a previously defined pattern, or click **New** and type a name for a new pattern. The following standard patterns are available:

- **KIWI Pattern** - Parses a basic KIWI Syslog Server file format

- **NetSight Syslog Pattern** Parses files generated by the Extreme Management Center Syslog Service

- **NetSight Trap Log Pattern** - Parses files generated by the snmpTrapd Service

- **UNIX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service

- **Console 1.x Pattern** - Parses files generated by Console 1.x

- **NetSight Log Pattern** - Parses files generated by Console and the other Extreme Management Center applications

- **1X Plugin Pattern** - Parses files generated by other Extreme Management Center applications

- **Red Hat LINUX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service

- **Ubuntu LINUX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

Fields

This table lists the field types that identify the column in which a particular element of parsed information should be placed. You can double-click a field type to add it to the pattern (or use the arrow button) or you can type field types directly into the pattern. Selecting a field type full pattern is enclosed within angle brackets (< , >) to signify beginning and end. A newline (\n) is assumed at the end in this case, but could be made required using a delimiter character. Field types within percentage symbols represent the column in which a piece of parsed information should be put. The following field types are available:

- %pri% = Priority string

- %pdate% - Parsed Date - Console is capable of interpreting several date formats. Use this field with %ptime% for most standard date/time formats. If this does not present the date correctly, use the following fields to parse the individual elements in the date.

- %date% - parses date elements and places the parsed information into the Date/Time column.

- %month%, %day%, %year% - separately parsed date elements. The parsed results are placed in the Date/Time column.

- %ptime% - Parsed Time - Console is capable of interpreting several time formats. Use this field with %pdate% for most standard date/time formats. If this does not present the time correctly, use separate fields to parse the individual elements in the time.

- %time% - parses the time elements and places the parsed information into the Date/Time column.

- %hour%, %min%, %sec%, %ampm% - separately parsed time elements. The parsed results are placed in the Date/Time column.

- %cat% - Category provides a means for sorting events (e.g., Poller, Application, Error)

- %sev% - Severity

- %user% - Username associated with the event.

- %ip% - Host IP Address associated with the event.

- %type% - Type (Event or Trap)

- %event% - a more specific keyword/phrase (i.e. "Contact Lost", "Contact Established")

- %info% - The information string.

- %discard% - information that is not used. This is information that is skipped over to parse the next piece.

Delimiters

This table lists the characters that are used in the selected file to separate information types. You can double-click a delimiter to add it to the pattern (or use the arrow button) or you can type a delimiter directly into the pattern. The list contains two types of whitespace delimiters (\w for whitespace and \t for tab). Use the \t when a single tab separates elements in the sample line. Whitespace can be used when the separator in the sample line is a tab, a series of tabs or series of spaces. Reserved characters must be preceded by a backslash (\)., The following delimiters are available:

- **\r** - return
- **\t** - tab
- **\n** - new line
- **\w** - whitespace

- **,** - comma

- **.** - period

- **:** = colon

- **;** - semicolon

- **-** - dash

Pattern

Displays the selected **Fields** and **Delimiters** that determine how each data element in the sample line will be parsed and placed in a column in the Event View.

Sample Log Line

This is a sample of raw log information.

Parsed

This table shows how the information will be presented in the Events tab. Cells are filled with the sample line information as field types are selected and delimited.

New Button

This button places a default name into the name field and clears the Pattern field, allowing you to define a new pattern. You can swipe the default name and type a name of your own choosing.

Delete Button

This button removes the currently selected pattern.

Apply Button

Applies the current pattern to the Pattern Name, but leaves the window open to allow creating/modifying another pattern.

OK Button

Applies the current pattern to the Pattern Name and closes the window.

Related Information

For information on related windows:

- [Event Manager Window](#)

- [Log Manager Parameters Window](#)

- [New Log Manager Window](#)

For information on related tasks:

- [How to Configure Events](#)

Open Log File Window

This window lets you select a log file from either the client or server for viewing in the Event Log Viewer window. It also lets you select the format used to parse the information presented in the Event Log Viewer. You can access this window from the **Open Event Log** button ![icon] in the lower-right corner of the Event View.

You can open an event log from the local Extreme Management Center client or from the Extreme Management Center Server. Both browsers offer several parsers to interpret the log information.

Event Log Parser

This drop down list lets you select a Pattern that will be used to interpret the log information presented in the Event Log Viewer window. The following standard patterns are available:

- **KIWI Pattern** - Parses a basic KIWI Syslog Server file format
- **NetSight Syslog Pattern** Parses files generated by the NetSight (Extreme Management Center) Syslog Service
- **NetSight Trap Log Pattern** - Parses files generated by the snmpTrapd Service
- **UNIX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service
- **Console 1.x Pattern** - Parses files generated by Console 1.x
- **NetSight Log Pattern** - Parses files generated by Console and the other NetSight (Extreme Management Center) applications
- **1X Plugin Pattern** - Parses files generated by other NetSight (Extreme Management Center) applications
- **Red Hat LINUX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service
- **Ubuntu LINUX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

Open Local Event Log

This browser opens with the default path set to the `<install directory>\clients` directory.

Sample File Browser Window
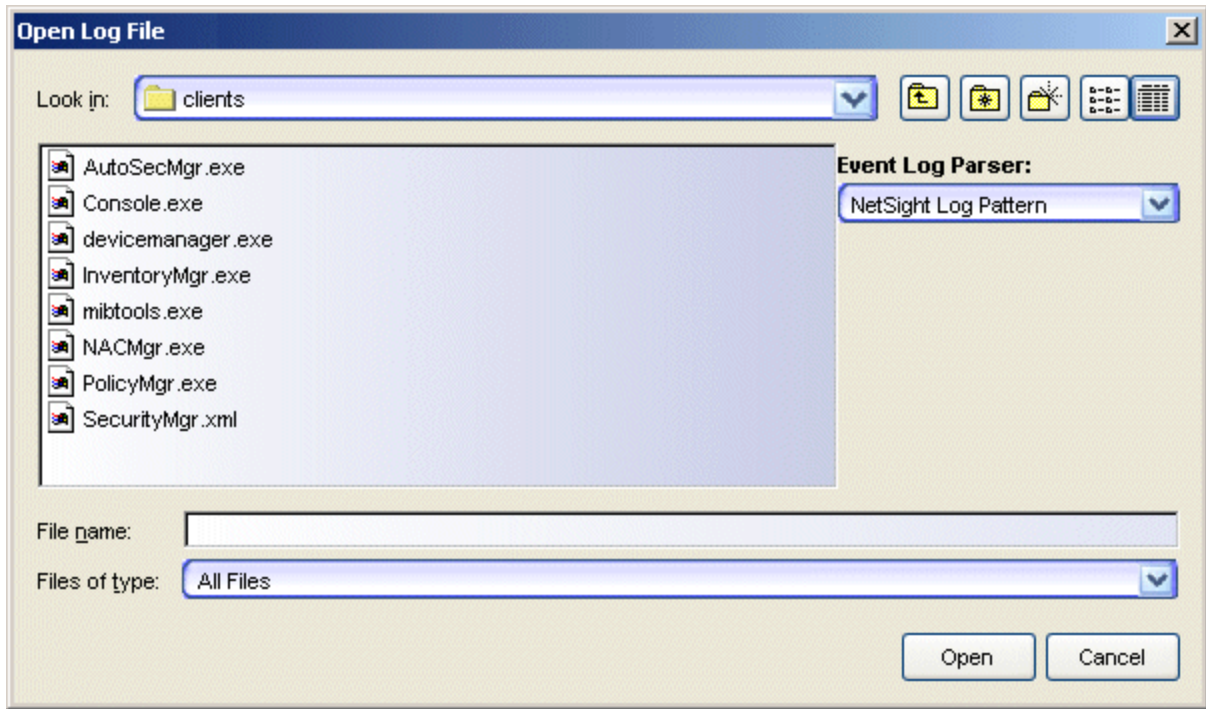
Open Event Log on Server

This browser opens with the default path set to the `<install directory>\appdata\logs` directory.

Sample File Browser Window
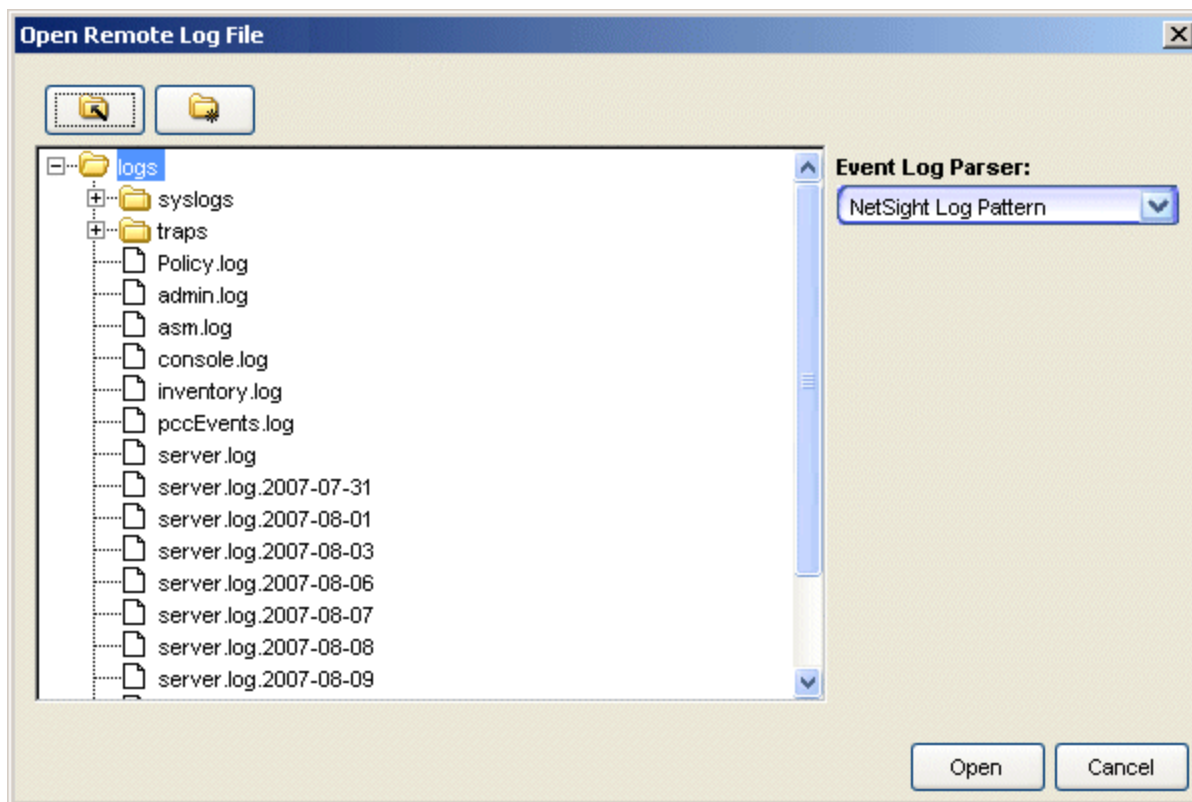
Related Information

For information on related windows:

- [Event Log Viewer](#)
- [Event View](#)
- [Event View Manager Window](#)

For information on related tasks:

- [How to Configure Events](#)

How to Configure Events in Extreme Management Center (Legacy)

You can use the Event View Manager window to add your own views (tabs) to the Event View panel. You can create custom tables that capture and combine similar information (same log type) from various sources. For example, you can combine or merge trap logs into a single Event View.

Instructions for:

- Creating a New Event View
- Modifying an Existing Event View
- Removing an Event View

Creating a New Event View

You can create custom tables that capture and combine alarms, events and/or traps from various sources to provide the information needed to manage your network in Extreme Management Center.

1. Click the Event View Manager button ⚙ in the lower-right corner of the Event View. (If you are using Console, you can also go to the **Tools** menu and select **Alarm/Event > Event View Manager**.) The Event View Manager window opens.

2. Click **Add** in the top panel. The New View window opens.

3. Type a **Name** for your new view. The name can be up to 32 characters long. Spaces and special characters are not permitted. This is the name that will appear on the tab for your new view in the Event panel.

4. Check one or more standard columns (**System Name**, **System Location**, **System Description**) to add those columns to your new view or check **Custom** to add custom columns. Custom columns can be added for any column from the **NSDEVICES** table. The NSDEVICES table can be found in the **NsSchema.xml** file which is located in the `<install directory>\jboss\server\default\deploy\NetSight\common\nscoreapi.jar` jar file. Within the jar file, the path is `com\enterasys\netsight\api\Resources\NsSchema.xml`.

   One or more columns can be defined as a comma delimited string using the

following format:

objName.objField:columnName

where:

objName.objField is the field name from the NSDEVICES table.
columnName is the name that will appear as the column heading.

For example:
chassisID:Chassis

NOTE: Device data in the Event View is not dynamically updated as the device's data changes. You will need to Refresh the Event View in order to see any changes.

---

5. Click **OK**. Your new tab name now appears in the **Title** column of the **Views** table. The **Log Managers** column is blank.

6. If the Available Log Managers table lists a log that you want to add to this tab, select that log manager from the list and click [icon]. The selected log manager is added to the **Log Managers in View** table and in the Log Managers column in the Views table.

7. If the desired log is not in the Available Log Managers table, you can add a log manager to the table, then add it to the **Log Managers in View** table. To add a new Log Manager

   a. Click **New**. The **Log Manager Parameters - New Log Manager** window opens.

   b. Type a name for your new Log Manager.

   c. Enter the path and filename for the log being managed by this Log Manager into the **Log File** field or click **Browse** to open a file browser where you can navigate and select a log file.

   d. If you are selecting a Syslog file, select a **Pattern** from the drop-down list to be used to interpret the information from the log file. You can select a currently defined pattern or click the **Config** button to open the Custom Pattern Configuration window where you can create a new pattern to match a format that is not parsed by one of the default pattern definitions:

- **KIWI Pattern** - Parses a basic KIWI Syslog Server file format

- **NetSight Syslog Pattern** Parses files generated by the NetSight (Extreme Management Center) Syslog Service

- **NetSight Trap Log Pattern** - Parses files generated by the snmpTrapd Service

- **UNIX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

- **Console 1.x Pattern** - Parses files generated by Console 1.x

- **NetSight Log Pattern** - Parses files generated by Console and the other NetSight (Extreme Management Center) applications

- **1X Plugin Pattern** - Parses files generated by other NetSight (Extreme Management Center) applications

- **Red Hat LINUX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

- **Ubuntu LINUX Syslog Pattern** - Parses files generated by the built-in UNIX/LINUX Syslog Service

    e. Click **OK** to add your new log manager to the Available Log Managers table and close the window.

8. With your new log manager selected, click [➡].

9. When you are satisfied with the list of log managers, click **Apply** to save your newly configured Event View.

10. Repeat Steps 2 through 9 to create another tab. Otherwise, click **OK** to exit from the Event View Manager window.

Modifying an Existing Event View

The mechanism for modifying an existing Event View is similar to creating a new one. The tab being modified is selected from the top panel and changes are applied in the two bottom panels.

To modify an existing Events Tab:

1. Click the Event View Manager button [icon] in the lower-right corner of the Event View. (If you are using Console, you can also go to the **Tools** menu and select

Alarm/Event > Event View Manager.) The Event View Manager window opens.

2. Select the View being changed from the list in the top panel.

3. Click **Edit** in the top panel to open the Edit View window where you can change the name of the View and add columns to the view. For information on adding custom columns, see step 4 above.

4. If the Available Log Managers table lists a log that you want to add to this tab, select that log manager from the list and click [→]. The selected log manager is added to the **Log Managers in View** table and in the Log Managers column in the Views table.

5. If the desired log is not in the Available Log Managers table, you can add a log manager to the table, then add it to the **Log Managers in View** table. To add a new Log Manager

   a. Click **New**. The **Log Manager Parameters - New Log Manager** window opens.

   b. Type a name for your new Log Manager.

   c. Enter the path and filename for the log being managed by this Log Manager into the **Log File** field or click **Browse** to open a file browser where you can navigate and select a log file.

   d. If you are selecting a Syslog file, select a **Pattern** from the drop-down list that will be used to interpret the information from the log file. You can select a currently defined pattern or click the **Config** button to open the Custom Pattern Configuration window where you can create a new pattern to match a format that is not parsed by one of the default pattern definitions:

      - **KIWI Pattern** - Parses a basic KIWI Syslog Server file format

      - **NetSight Syslog Pattern** Parses files generated by the NetSight (Extreme Management Center) Syslog Service

      - **NetSight Trap Log Pattern** - Parses files generated by the snmpTrapd Service

      - **UNIX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service

      - **Console 1.x Pattern** - Parses files generated by Console 1.x

      - **NetSight Log Pattern** - Parses files generated by Console and its current plugins

      - **1X Plugin Pattern** - Parses files generated by Console 1.x plugins

- **Red Hat LINUX Syslog Pattern** - Parses files generated by the built in UNIX/LINUX Syslog Service

  e. Click **OK** to add your new log manager to the Available Log Managers table and close the window.

6. With your new log manager selected, click .

7. When you are satisfied with the list of log managers, click **Apply** to save your newly configured Event View.

8. Repeat Steps 2 through 6 to modify another view. Otherwise, click **OK** to exit the Event View Manager window.

Removing an Event View

To remove an Event View from the Event View panel:

1. Click the Event View Manager button in the lower-right corner of the Event View. (If you are using Console, you can also go to the **Tools** menu and select **Alarm/Event > Event View Manager**.) The Event View Manager window opens.

2. Select the View being removed from the list in the top panel.

3. Click the **Remove** button.

Related Information

For information on related windows:

- Event View
- Event View Manager Window

LDAP Configuration

The Help topics in this section describe how to view and define the LDAP configurations used in your Extreme Management Center applications.

Add LDAP Configuration Window

Use the Add LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the Users/Groups tab in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by selecting New from the drop-down menu in the LDAP Configuration field. You can also access this window from the Manage LDAP Configurations window. Any changes made in this window are written immediately to the Extreme Management Center database.

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

Add LDAP Configuration ✖

Configuration Name: [   ]

LDAP Connection URLs

🗔 Add...   📝 Edit...   ⊖ Delete   ▲ Up   ▼ Down

Authentication Settings

Administrator Username: [   ]

Administrator Password: [   ] 👁

Timeout (seconds): [4   ] ▲▼

Search Settings

User Search Root: [   ]

Host Search Root: [   ]

OU Search Root: [   ]

Schema Definition

User Object Class: [person   ]

User Search Attribute: [   ]

Keep Domain Name for User Lookup: ☐

User Authentication Type: [LDAP Bind   ▼]

Test... | Populate Default Values

[**Save**] [Cancel]

Configuration Name

Enter a name for the LDAP configuration.

LDAP Connection URLs

Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) Use the Up and Down arrows to arrange the order that the URLs are listed.

The format for the connection URL is `ldap://host:port` where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port` and the default port is 636. For example, `ldaps://10.20.30.40:636`. If you are using LDAPS, your Extreme Management Center/Extreme Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.

If you are creating an LDAP configuration for Novell eDirectory, be aware that the eDirectory may require that the universal password lookup be done using LDAPS. If you configure the URL for LDAP only, the lookup may fail.

Authentication Settings

Enter the administrator username and password that will be used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server. The timeout field lets you specify a timeout value in seconds for the LDAP server connection.

Search Settings

For the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name).

Schema Definition

Provide information that describes how entries are organized in the LDAP server.

Schema Definition fields:

- **User Object Class** - enter the name of the class used for users.

- **User Search Attribute** - enter the name of the attribute in the user object class that contains the user's login ID.

- **Keep Domain Name for User Lookup** - If selected, this option will allow the full username to be used when looking up the user in LDAP. For example, you should select this option when using the User Search Attribute: userPrincipalName.

  If the option is not selected, the domain name will be stripped off the username prior to performing the lookup. For example, you should deselect this option when using the User Search Attribute: sAMAccountName. Two examples of the domain name being stripped off would be:
  user@domain.com -> user
  DOMAIN\user -> user

- **User Authentication Type** - Specify how the user is authenticated. There are 4 options:

  - LDAP Bind – This is the easiest option to configure, but only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types.

  - NTLM Auth – This option is only useful when the backend LDAP server is really a Microsoft Active Directory server. This is an extension to LDAP bind that uses ntlm_auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests.

  - NT Hash Password Lookup – If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Extreme Access Control read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request.

  - Plain Text Password Lookup – If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.

- **User Password Attribute** - This is the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.

- **Host Object Class** - enter the name of the class used for hostname.

- **Host Search Attribute** - enter the name of the attribute in the host object class that contains the hostname.

- **Use Fully Qualified Domain Name** checkbox - use this checkbox to specify if you want to use the Fully Qualified Domain Name (FQDN) or just hostname without domain.

- **OU Object Classes** - the names of the classes used for organizational units.

Test Button

The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user/host search that lets you search on a user entry or host entry value and display the attributes associated with those values.

Populate Default Values Button

Select from the defaults available from the menu:

- **Active Directory: User Defaults** - Settings that allow user authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.

- **Active Directory: Machine Defaults** - Settings that allow machine authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.

- **OpenLDAP Defaults -** Settings that allow Extreme Access Control to verify the user's password via an OpenLDAP server. See the NAC Manager How to Configure PEAP Authentication via OpenLDAP Help topic for information.

- **Novell eDirectory Defaults** - Settings that allow Extreme Access Control to read the universal password from Novell eDirectory. You must configure eDirectory to allow that password to be read. See the NAC Manager How to Configure PEAP Authentication via eDirectory Help topic for information.

Related Information

For information on related windows:

- [Manage LDAP Configurations Window](#)

LDAP Lookup Against AD using Lower Permissions in Extreme Management Center

This help topic provides instructions for configuring the minimum set of administrative privileges (permissions) that NAC Manager needs to authenticate to the Active Directory Server.

1. In Active Directory Users and Computers view, use the View menu to enable Advanced Features (View > Advanced Features).

2. Right-click on the Computers folder and select Properties from the menu.
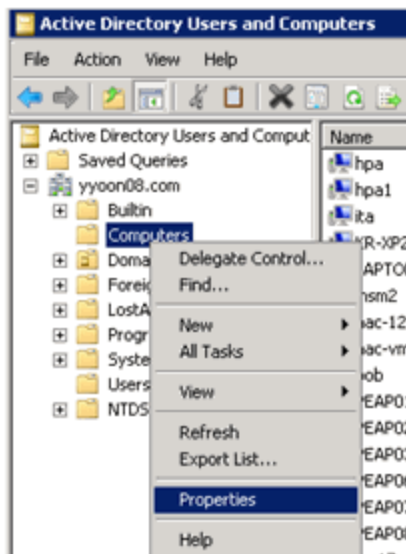
3. In the Computers Properties window, click the **Advanced** button to open the Advanced Security Settings for Computers window.
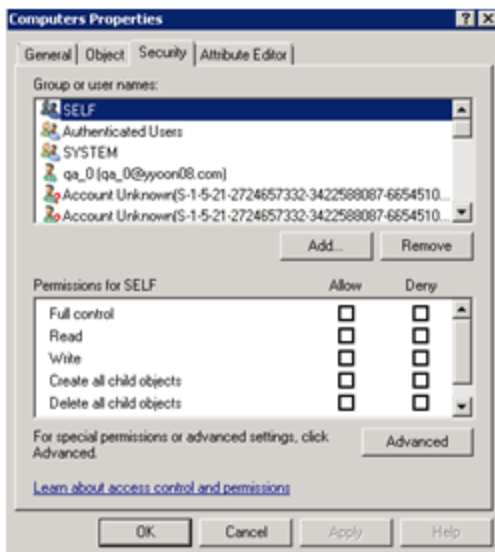
4. In the Permission entries section, click the **Add** button to add a new permission entry for a user.
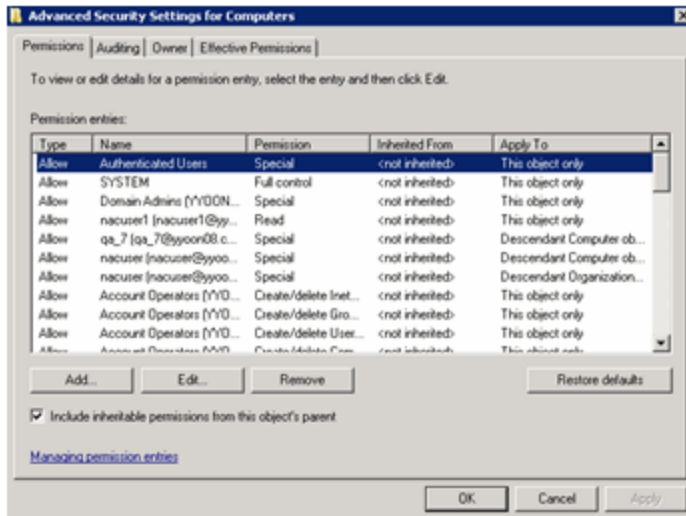
5. The Permission Entry for Computers window opens. In the "Apply to:" field, enter "Descendant Computer objects" (for Windows 2003, enter "Computer objects"). In

the Permissions section, select the Allow checkbox for Reset Password. Click **OK**.
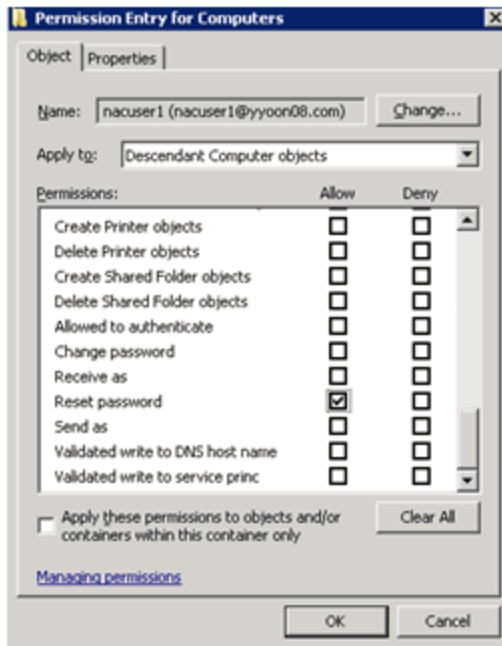
6. A new entry is created in the Advanced Security Settings for Computers window. Click **OK**.
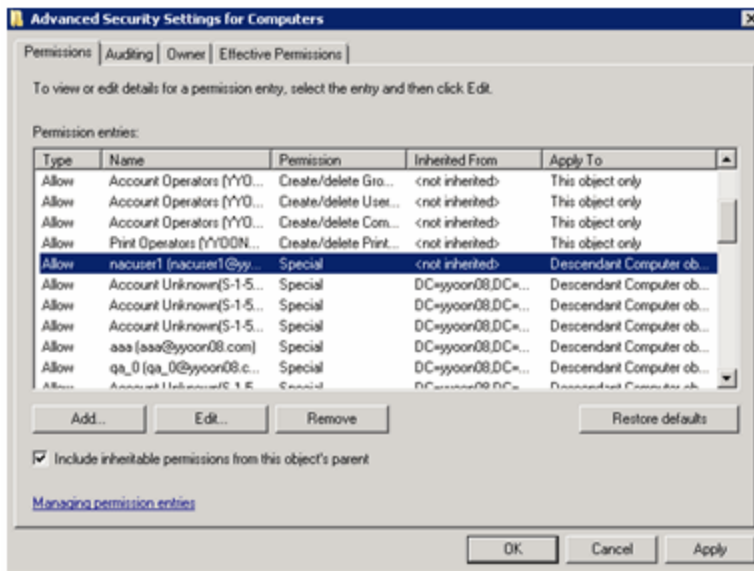
The permissions are now configured. You must now go to NAC Manager to configure your Advanced AAA Configuration. For more information, see the NAC Manager Help topic "How to Configure LDAP for End Users and Hosts via Active Directory".

Manage LDAP Configurations Window

This window lets you view and define the LDAP configurations used in your Extreme Management Center applications. You can access this window from the Users/Groups tab in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by clicking the drop-down menu in the LDAP Configuration field. Any changes made in this window are written immediately to the Extreme Management Center database.
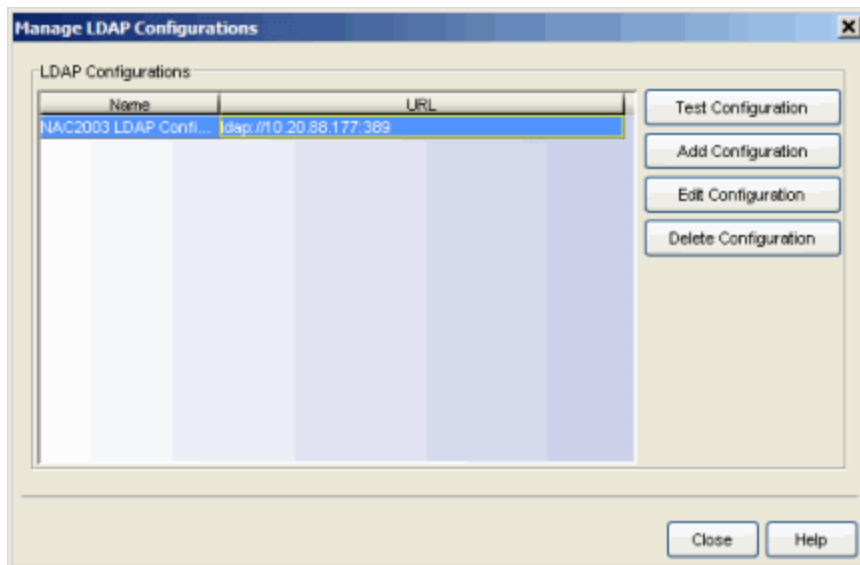
LDAP Configurations Table

The name of the configuration and the LDAP server connection URLs specified for that configuration.

Test Configuration Button

Use this button to run a connection test for the selected configuration. The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user search that lets you search on a user entry value and display the attributes associated with the user.

Add Configuration Button

Opens the Add LDAP Configuration window where you can define a new LDAP configuration.

Edit Configuration Button
> Opens the [Edit LDAP Configuration window](#) where you can edit the selected LDAP configuration.

Delete Configuration Button
> Deletes the selected LDAP configuration(s).

Related Information

For information on related windows:

- [Add/Edit LDAP Configuration window](#)

Failover with VMware® ESX™

This Help topic describes how to provide an Extreme Management Center server recovery plan for the Extreme Management Center [virtual engine](#) using the VMware ESX High Availability (HA) feature.

VMware HA is a feature that allows a [virtual machine](#) to be started on a new [host](#) within a [cluster](#), if the host that was executing it fails. The vCenter Server monitors the health of hosts in a cluster by sending heartbeat requests to each host. If a host does not respond within a configured interval, the vCenter server determines the host has failed and begin executing its virtual machine on a new host within the cluster. Once the virtual machine has been started on another host, it begins normal operation. Backups do not need to be restored, and there is no manual intervention required.

The Extreme Management Center Failover solution provides a recovery plan in the event of a host power or hardware failure (such as a hard disk, memory, or CPU failure). It does **not** provide a recovery plan for a Extreme Management Center server software failure.

With VMware HA, if the host executing a Extreme Management Center server crashes, the same Extreme Management Center server automatically appears again in a matter of minutes on another host. It retains the same hostname, IP address, and network configuration. There is interruption of service and activities that were in progress when the host crashed, but every transaction committed to disk persists, and most Extreme Management Center clients automatically reconnect when the server is back online.

This solution is a fully automated recovery process that doesn't require any user intervention or reliance on database backups, which can be hours or days old. It doesn't require a secondary server to be separately maintained and kept up-to-date, and it doesn't rely on administrators for either the detection or recovery of host failures.

NOTE: The Extreme Management Center Failover solution requires that vCenter Server is used to manage both hosts, and that the hosts are licensed for VMware HA.

The following sections discuss the hardware and software configuration requirements for this solution. Once configuration is complete, no user operation is required to recover from a host failure.

Instructions on:

- [Hardware Configuration](#)
- [Software Configuration](#)
- [Terminology](#)

Hardware Configuration

The following diagram shows a typical hardware configuration for the Extreme Management Center Failover solution using VMware's High Availability (HA) feature.
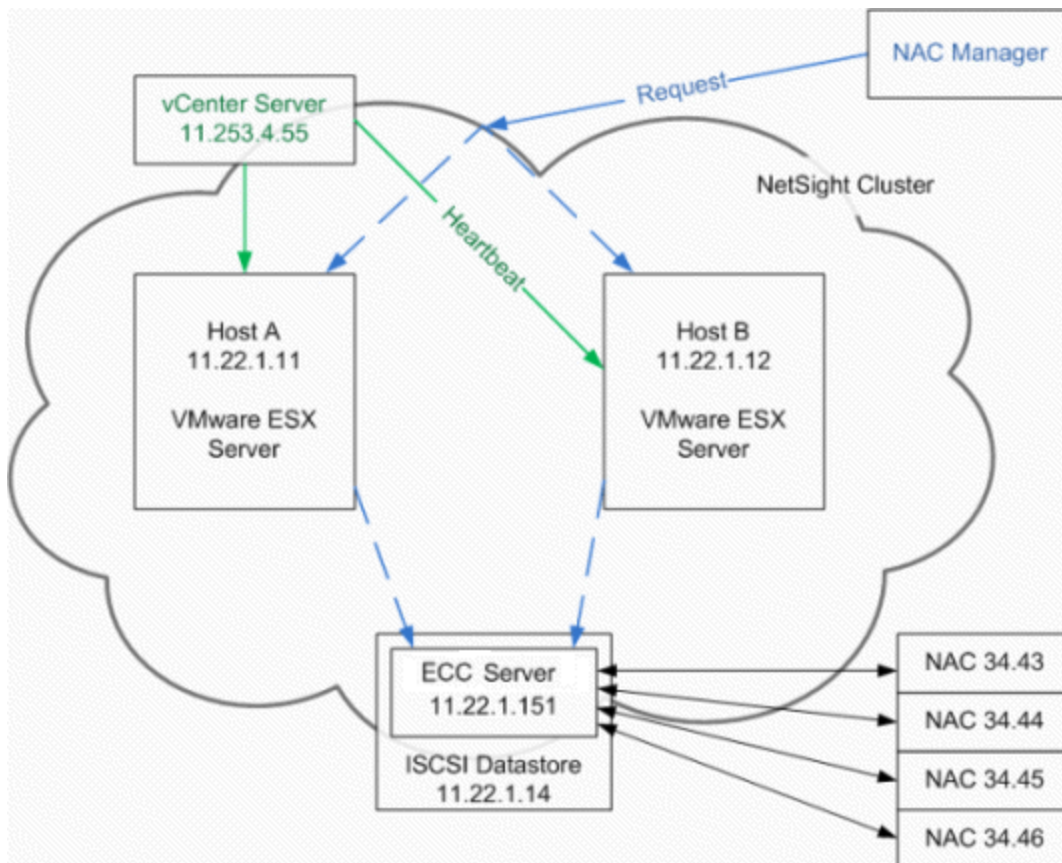
In this configuration, the vCenter Server is configured to manage the hosts in a cluster called "Extreme Management Center Cluster." There are two hosts with VMware's ESX server installed on them: Host A (11.22.1.11) and Host B (11.22.1.12). The vCenter Server is installed on a Windows server machine at 11.253.4.55. The vCenter Server is configured to send heartbeat requests to the hosts and

considers them failed if it does not hear a response within 30 seconds. Both hosts are configured with a common ISCSI datastore hosted on a Red Hat Linux box at 11.22.1.14 (however, other types of network storage can be used). The Extreme Management Center server is configured to manage four Extreme Access Control engines. The NAC Manager clients can be run on any machine.

The datastore is the persistent storage for the virtual machine. It is where the Extreme Management Center server software is installed, the configuration information is kept, and where the database tables are stored. The virtual engine code is executed on the host. When a host fails, the virtual engine execution moves to the other host and all of the data is maintained in the datastore. This allows the Extreme Management Center server to continue functioning without having to restore a database backup.

> **NOTE:** If there is a problem with network communication between the vCenter Server and the host, the vCenter Server may think the host is down when it is not. This is called Network Isolation. In this case, it is recommended that you shut down the virtual machine on the isolated host so that it will release any file locks on the shared datastore. Otherwise the replacement virtual machine on the second host may have trouble accessing the datastore. Refer to your VMware documentation for more information on Network Isolation.

Software Configuration

When using the VMware High Availability (HA) feature, your VMware environment must be configured to manage hosts in a cluster and the hosts must be licensed for VMware HA. There is no configuration required on the Extreme Management Center server to support the feature. If your VMware environment is already configured to take advantage of VMware HA, there is nothing additional that needs to be done to support it for the Extreme Management Center server.

Below is an example of what a cluster looks like in the VMware client. In this example, the cluster is named "BusinessCluster" and the Extreme Management Center server is shown as "NetSight Appliance 4.1."
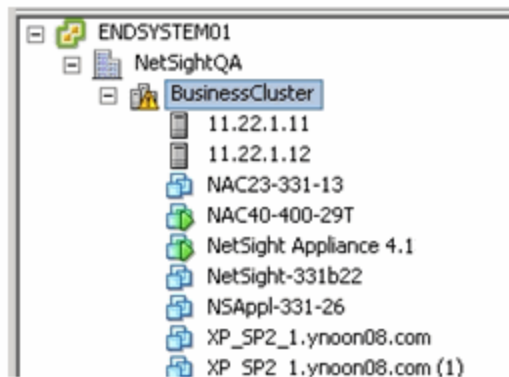
Once the licensed hosts are in a cluster, VMware HA can be enabled with a checkbox in the cluster's settings, as shown below. Refer to your VMware documentation for more information on configuring clusters.
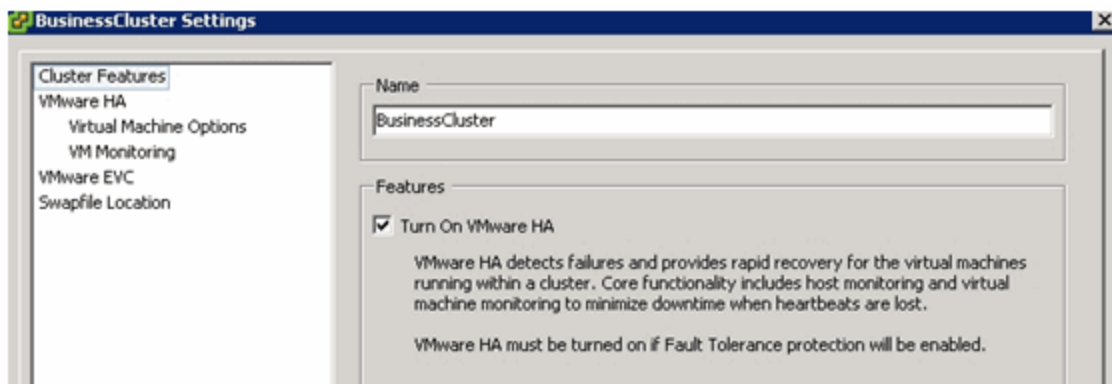
Terminology

Cluster

A cluster is a logical organization of hosts. It is used by VMware to group hosts for the purpose of supporting VMware HA and other VMware features.

Datastore

A datastore is any network storage accessible by a VMware server (local or remote). The datastore is often broken into pieces for use by the virtual machines as simulated hard drives.

Host

A host is the physical computer that is running the VMware server software.

Virtual Appliance

> A virtual appliance is a prepackaged virtual machine that has an operating system and dedicated software already installed on it.

Virtual Machine

> A virtual machine refers to the simulated computer instance running inside the VMware server.

Using the Help System

All Extreme Management Center documentation is available in this online help system. Online help is available from the Help menus and Help buttons throughout Extreme Management Center and all legacy java applications.

Accessing Help

There are several ways to access the help system:

- Extreme Management Center — Select the **Help** button (?) in the top right corner of your browser.
- Legacy java applications — Select the **Help > Help Topics** menu option. For help on the tab currently displayed in the right panel of the application main window, select the **Help > About This Window** menu option.

The Extreme Management Center Online Help opens in a frame to the right of the main Extreme Management Center window.

Help Features

The help is context-sensitive and as such, the topic displayed in the right panel changes as you navigate Extreme Management Center. To prevent the help topic from changing when you change screens in Extreme Management Center, click the **Pause** button ( ) at the top of the help window.

A left panel is available to assist you with navigation of the help by clicking the **Show Navigation** button ( ).

To open the help in a separate tab, click the **Launch Help** button ( ). The left panel contains the Table of Contents. Items with a **>>** indicate that clicking the TOC item opens another menu of options.

The Help toolbar also contains buttons search all topics.

Use the **Search** bar (Search) and then click the **Magnifying** glass button (Q) to search for a word or phrase in the help. If you want to find a

specific combination of words that are always next to each other in the same order, enter the search keywords within quotation marks (for example, "domain name"). The Search feature lets you refine the Search results by using the **Filter** button ( ). Clicking it opens a pop-up menu displaying certain areas of the documentation to which you can limit your results.

Searching Within Topics

To search for specific instances of a term in only the currently accessed help topic, type **Ctrl** + **F** to open your browser's search box. Use this to search for the term or phrase in the currently accessed help topic.

Services

When you install Extreme Management Center on a Windows or Linux system, you have the option of enabling (configuring to launch automatically) the Extreme Management Center Services.

NOTE: If you have performed a silent Linux installation or installed Extreme Management Center on the Extreme Management Center hardware or virtual engine, the Extreme Management Center Services are automatically enabled.

The services offered depend on whether your platform is Windows or Linux.

- **SNMPTrap Service** (Windows and Linux) - Enables SNMP trap messages to be received and logged when problems or irregularities are detected on network devices. Only one trap service may be running at a time on a server. If you are also running a network management system on the server, you may wish to use the network management trap service.

- **TFTP** (Windows and Linux) - Enables you to upload and download configuration files, and download firmware to devices. Only one TFTP service may be running at a time on a machine.

  NOTE: The Extreme Management Center TFTP Service does not support IPv6.

- **BOOTP** (Windows only) - Enables the Extreme Management Center server to also be a BOOTP server. This allows the server to supply devices with firmware images (or other basic identity information) in the event the device's current firmware image becomes corrupt. Only one BOOTP service can be running at a time on a machine.

- **Syslog** (Windows only) - Extreme Management Center Console maintains a record of syslog messages in the Syslog tab of the Event View.

When you enable a Extreme Management Center service, it runs in the background on the workstation. The service starts automatically by default, and if you shut down and restart the workstation, the service is restarted automatically.

There may be times when you want to stop or restart the services manually. For Windows users, Extreme Management Center provides a Services Manager that shows you which of the services are running, and lets you stop, start, or restart

them individually or all at once. You can also stop and start the Services Manager itself.

In addition, if you are not using a service, you may want to disable the service completely so that it does not start automatically if you restart the system.

The instructions below explain how to manually stop, start, or disable a Extreme Management Center service, and how to stop and start the Services Manager on Windows systems.

Instructions on:

- Stopping and Starting Extreme Management Center Services

  - Windows

  - Linux

- Disabling an Extreme Management Center Service

  - Windows

  - Linux

- Stopping and Starting the Services Manager (Windows Only)

Stopping and Starting Extreme Management Center Services

The information in this section provides instructions for stopping and starting a service manually on Windows and Linux platform systems.

Windows

You can manually start, restart, or stop Extreme Management Center services individually or all at once. On a Windows platform system:

1. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar).

2. Locate the Services Manager icon ( ) and right-click it. (If you don't see the icon, you can start the Services Manager from the **Start > Programs** or **All Programs** menu; select **Startup > Services Manager**.)

3. Select the appropriate menu option. Menu options that are not currently available for the service(s) are grayed out.

- **Start** - Starts a service that is not currently running.

- **Restart** - Stops a service that is currently running, and starts it up again immediately.

- **Stop** - Stops a service that is currently running.

- **Start automatic services** - Starts any services that have been enabled (configured to launch automatically via selection at installation or in the [Services for Extreme Management Center Server window](#)).

- **Restart running services** - Stops all services that are currently running, and starts them up again immediately.

- **Stop running services** - Stops all services that are currently running.

- **Exit** - Stops all currently running services and shuts down the Services Manager.

Linux

You can manually start, restart, or stop Extreme Management Center services individually. Restarting a service stops a service that is currently running, and starts it up again immediately. You can also use the status option to determine if a service is running.

On a Linux platform system:

1. Navigate to the /etc/init.d directory.

2. Type the service name, a space, and either **start**, **restart**, **stop**, or **status** depending on what you want to do, and press **Enter**. These are the service names to use:

- SNMP trap service - nssnmptrapd

- TFTP service - nstftpd

- Extreme Management Center Server - nsserver

- Extreme Management Center Database - nsdatabase

For example, to stop the SNMP trap service, type:
`nssnmptrapd stop`
and press **Enter**.

To determine whether or not the SNMP trap service is running, type:

```
nssnmptrapd status
```
and press **Enter**.

On a Extreme Management Center Engine or Extreme Management Center Virtual Engine:

1. Navigate to the /etc/rc.d directory.

2. Type the service name, a space, and either **start**, **restart**, **stop**, or **status** depending on what you want to do, and press **Enter**. These are the service names to use:

    - SNMP trap service - rc.nssnmptrapd

    - TFTP service - rc.nstftpd

    - Extreme Management Center Server - rc.nsserver

    - Extreme Management Center Database - rc.nsdatabase

    For example, to stop the SNMP trap service, type:
    ```
    rc.nssnmptrapd
    ```
    and press **Enter**.

Disabling an Extreme Management Center Service

When a Extreme Management Center service is enabled during installation, it restarts automatically if the system is restarted, even if it has been manually stopped. If you are not using a service, in order to prevent the service from automatically restarting during a system restart, you must disable it.

There are several reasons you might want to disable a Extreme Management Center service if it is not being used. For example, disabling an unused service can avoid possible port conflicts and conserve system resources. In addition, some installations might require disabling unused services as part of their security process.

The information in this section allows you to disable a service without uninstalling it.

Windows

To disable a Extreme Management Center Service on a Windows platform system:

1. Open the Windows Control Panel.

2. Navigate to Administrative Tools > Services.

3. In the Services window, double-click on the Service entry. A Properties window opens.

4. On the **General** tab, set the Startup type to either **Manual** (if you want to allow the service to be started manually) or **Disabled** (if you want to completely disable the service). If you are turning off the service for security purposes you should set the Startup type to **Disabled**.

5. Click **OK**.

Linux

Use the following commands to enable or disable a Extreme Management Center Service on a 64-bit hardware or virtual Extreme Management Center engine.

1. Navigate to the /etc/rc.d directory.

2. Type the command update-rc.d, the service name, and either **enable** or **disable**, and press **Enter**. These are the service names to use:

   - SNMP trap service - nssnmptrapd

   - TFTP service - nstftpd

   For example, to disable the SNMP trap service, type:
   update-rc.d nssnmptrapd disable
   and press **Enter**.

   To enable the TFTP service, type:
   update-rc.d nstftpd enable
   and press **Enter**.

Stopping and Starting the Services Manager (Windows Only)

The Extreme Management Center Services Manager runs on the Windows platform only.

Stopping

Stopping the Services Manager stops all running Extreme Management Center services.

1. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated it).

2. Locate the Services Manager icon ( ) and right click it.

3. Select **Exit** from the menu.

Starting

The Extreme Management Center Services Manager automatically starts for the user that performed the Extreme Management Center installation. You can manually start the Services Manager using the following instructions. Starting Services Manager starts all Extreme Management Center services enabled at installation or via the **Tools > Options** Services for Extreme Management Center Server window.

1. From the **Start > Programs** or **All Programs** menu, select **Startup > NetSight (Extreme Management Center) Services Manager**.

Suite-Wide Options (Legacy)

Suite-wide options apply across all Extreme Management Center applications. You can set suite-wide options using the Options window accessed from the **Tools > Options** menu in any application.

How to Set Suite Options in Extreme Management Center (Legacy)

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 select 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](#)
- [Extreme Management Center Feedback Program](#)
- [Extreme Management Center Server Health](#)
- [Network Monitor Cache](#)
- [Port Monitor](#)
- [Services for Extreme Management Center 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 Extreme Management Center Server use the MyMibs directory or thirdparty directory.

The MyMibs directory is where you add proprietary MIBs to the MIB database on the Extreme Management Center Server. This MIB information is then distributed to the Extreme Management Center remote clients. If you select this option, the Extreme Management Center Server also uses the MyMibs directory (e.g. the MIBs are 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 Extreme Management Center Server also uses the third party directory.

CAUTION: In most situations, it is recommended the Extreme Management Center Server does **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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center Server for these settings to take effect.

Advanced Suite Settings

The [Advanced Suite Settings view](#) provides the option to enable or disable Extreme Management Center Suite Beta Features. A list of the beta features can be found in the Extreme Management Center Suite Release Notes. When you enable the Beta features, you are asked for a Beta Activation Key. Contact Extreme Networks Support to obtain a Beta Key. Once you enable the beta features, the button changes to "Disable Beta Features."

This option applies to all users. For this setting to take effect, the Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 are 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 are also recorded.

Preserve Triggering Events in Alarm History – This option preserves alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by clicking the View Trigger button in the Alarm History window.

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 Extreme Management Center 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 Extreme Management Center 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>\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>\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 Extreme Management Center 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 user disconnects. This option specifies a duration of end user inactivity (no keyboard or mouse activity) before the user is disconnected from the Extreme Management Center

Server. If this option is enabled, after the specified amount of time, the end user is disconnected from the Extreme Management Center Server and the application closes. This option applies to the current logged-in user. You must be a member of an authorization group 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 Extreme Management Center 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. 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 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. 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 Extreme Management Center 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 Extreme Management Center reporting data. Because the alarm and reporting databases can be quite large, this allows you to control the amount of disk space used by the database backup operation.

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 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 Extreme Management Center 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 Extreme Management Center applications and various Extreme Management Center 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 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.

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 NAC 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 Extreme Management Center Server to clear the old credentials from the cache. Click **OK**.

> **NOTE:** The update procedure uses these proxy settings only when necessary, otherwise the settings are ignored.

6. 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 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 Extreme Management Center. 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=10.20.1.2 server = 10.20.1.1". 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. 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. The first time the hostname cache service is started, if the Local address domains list has not been defined, Extreme Management Center attempts to auto-populate it by resolving the IP address of the Extreme Management Center server. If it resolves to a subdomain, Extreme Management Center creates 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.

Extreme Management Center Feedback Program

This option allows you to enable or disable participation in the Extreme Management Center Customer Feedback Program. If you participate, Extreme Management Center gathers anonymous usage information used to better understand how Extreme Management Center 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 Extreme Management Center that automatically upload troubleshooting information, and more.

The information gathered will not be used for marketing purposes or to contact you.

Setting Extreme Management Center Server Health Options

Use the NetSight (Extreme Management Center) Server Health view to select an option to send an email if the Extreme Management Center 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 increases background SNMP performed by the server.

Storing this information greatly improves performance for views in Extreme Management Center that request the data. Leave the cache 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 Extreme Management Center 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 displays 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 displays 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 Extreme Management Center Server Options

Use the Services for NetSight (Extreme Management Center) 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 Extreme Management Center TFTP server or another TFTP server. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server 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 Extreme Management Center TFTP service, keep in mind the following requirements when setting the path to your root directory:

- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.

- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive (e.g. C:\ or D:\).

- If you are using a TFTP server on a remote system, use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (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 Extreme Management Center E-Mail notification feature. The E-Mail notification feature is used in Console's alarm action configuration and in Inventory Manager's Capacity Planning report scheduling. 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 Extreme Management Center 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 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 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 Extreme Management Center to use when launching web pages from Extreme Management Center 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 Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8080 (HTTP) and 8443 (HTTPS). If you change the port ID, you must restart the Extreme Management Center 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 Extreme Management Center web-based views, such as Extreme Management Center web pages and the legacy Console java application's FlexViews.

5. The Password AutoComplete 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 NAC Manager 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](#)

Suite Options Window (Legacy)

Suite options apply across all Extreme Management Center applications. In the Options window (**Tools > Options**), the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Suite folder to view the suite-wide options you can set.

Information on 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](#)
- [Extreme Management Center Feedback Program](#)
- [Extreme Management Center Server Health](#)
- [Network Monitor Cache](#)
- [Port Monitor](#)
- [Services for Extreme Management Center Server](#)
- [SMTP E-Mail Server](#)
- [Status Polling](#)
- [System Browser](#)
- [Trap Configuration](#)

- [Tree](#)

- [Web Server](#)

Advanced SNMP Settings

Selecting Advanced SNMP Settings in the left panel of the Options window provides the following view where you can elect to have the Extreme Management Center Server use the MyMibs directory or thirdparty directory.

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 Console retries a timed-out request three time after the initial attempt at contact is made, making a total of four attempts to contact a device. The value for this setting must be between 1 and 60 tries.

> You can override this value on a per-device basis by highlighting a device in the Console device tree, accessing the **Properties** tab, and selecting the **Access** radio button. Enter the override value for the selected device in the [Retries column](#).

Length of SNMP Timeout (in seconds)

> The amount of time (in seconds) that Console waits before re-trying to contact a device. The default setting is 5 seconds. The value for this setting must be between 3 and 60 seconds.
>
> You can override this value on a per-device basis by highlighting a device in the Console device tree, accessing the **Properties** tab, and selecting the **Access** radio button. Enter the override value for the selected device in the **Timeout column**.
>
> **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.

The MyMibs directory is where you add proprietary MIBs to the MIB database on the Extreme Management Center Server. This MIB information is then distributed to the Extreme Management Center remote clients. If you select this option, the Extreme Management Center Server also uses the MyMibs directory (e.g. the MIBs will be included in the SNMP Server Stack).

The thirdparty 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 Extreme Management Center Server will also use the thirdparty directory.

> **CAUTION:** In most situations, it is recommended that the Extreme Management Center 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 Extreme Management Center 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.
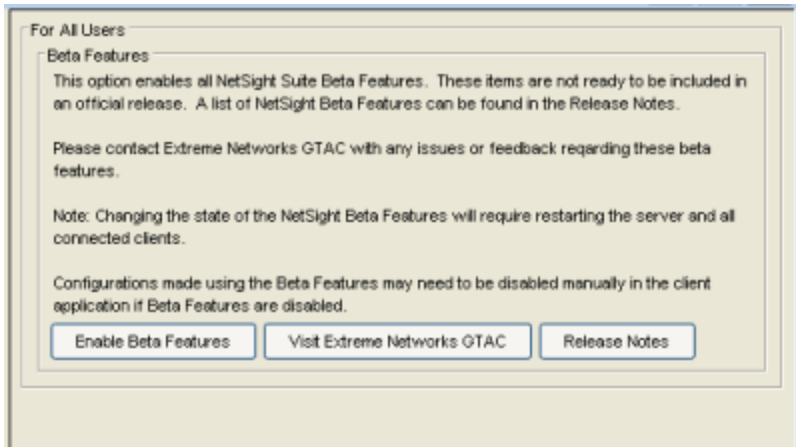
These options apply to all users. For these setting to take effect, the Extreme Management Center Server must be restarted.

Advanced Suite Settings

Selecting Advanced Suite Settings in the left panel of the Options window provides the following view where you can enable or disable Extreme Management Center Suite Beta features. A list of the beta features can be found

in the Extreme Management Center 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 Extreme Management Center Server must be restarted.

Alarm Configuration

Selecting Alarm Configuration in the left panel of the Options window provides the following view where you can configure options for how alarms are handled on your network. These settings apply to all users.

Consolidate Email Option

This option allows you to 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.

Alarm Optional Features

The **Enable Sender Overrides** option adds 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.

Alarm History

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.

Alarm Action Defaults

Use this section to define the default content for 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.

Following is a list of the most common keywords used. For a complete list of available Alarms Manager keywords, see the Edit Action Overrides window in the Console online Help.

- $alarmName – the name of the alarm.
- $severity – the alarm severity.
- $deviceIP – the IP address of the device that is the source of the alarm.
- $message – the event message.
- $time – the date and time when the event or trap occurred.

E-Mail Subject

Defines the text that will be included in the e-mail subject line.

E-Mail Body

Defines the text that will be included in the e-mail body.

Syslog Tag

Defines the string used to identify the message issued by the syslog program.

Syslog Message

Defines the text that will be included in the syslog message.

Trap OID

The OID that defines the trap.

Trap Message

The varbind that is sent in the trap.

Trap Message OID

The OID of the varbind being sent that represents the message.

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.

Advanced Settings

Click the Advanced Settings button to open the Alarm Advanced Settings window where you can set advanced alarm options.

Alarm/Event Logs and Tables

Selecting Alarm/Event Logs and Tables in the left panel of the Options window 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 more information on configuring log files, see the Extreme Management Center Log Files Help topic in the Console online Help.

Number of Event logs to limit

> This option lets you limit the number of application log files that are saved to the `<install directory>\appdata\logs` directory. It does not limit the number of Traps or Syslog logs that are saved. Specify 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** – 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.

Number of Server logs to limit

> A new server log is created every day. This option lets you limit the number of server log files that are saved to the `<install directory>\appdata\logs` directory. Specify one of the following options:

- **Do not limit the number of server log files saved** -- Allows you to keep all server log files.

- **Limit the number of server 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.

Number of Rows to keep in Event and Alarm table

These settings determine the number of table rows that will be displayed in all of the logs in the Alarm View and the Event View (in the Console main window). 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.

Clip to *nnnn* **rows**

This value sets the number of rows that will remain in the table when the clip limit is exceeded.

Clip when above is exceeded by *nnnn* **rows**

This value, added to the **Clip to** *nnnn* **rows** setting determines when the table will be clipped (trimmed to the value of **Clip to** *nnnn* **rows**).

Event Log entry timestamp 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.) 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.

Event and Alarm Table Host/Port Names

These options let you configure host name and port name resolution, and display the device hostname in the Source column in alarm and event tables:

- **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.)

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.

Client Connections

Selecting Client Connections in the left panel of the Options window provides the following view where you can configure client connection options.
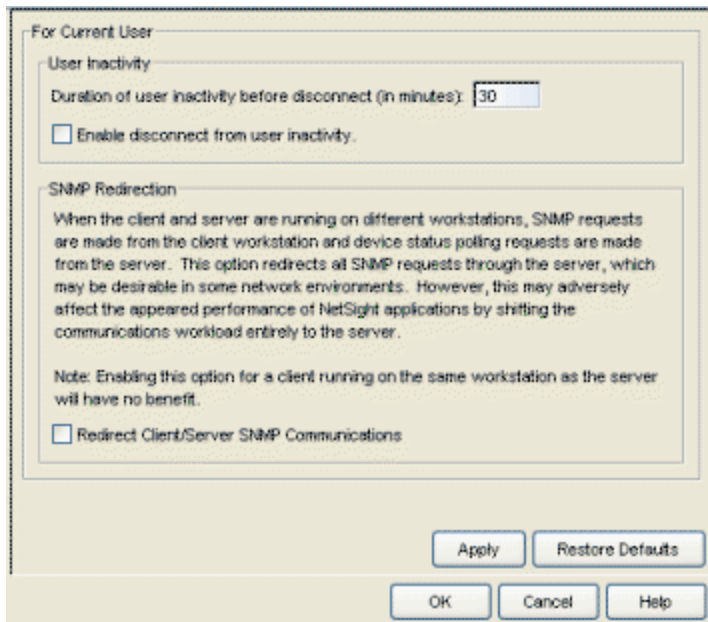
User Inactivity

This option specifies a duration of end user inactivity (no keyboard or mouse activity) before the user will be disconnected from the Extreme Management Center Server. If this option is enabled, after the specified amount of time, the end user is disconnected from the Extreme Management Center Server and the application

closes. This option applies to the current logged-in user. You must be a member of an authorization group assigned the Server Information > Disconnect Clients capability to configure this option.

SNMP Redirection

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 Extreme Management Center 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.

Database Backup

Selecting Database Backup in the left panel of the Options window provides the following view where you can schedule backups of the Extreme Management Center database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all Extreme Management Center applications is saved and readily available, if needed.

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.

You can also specify whether to save all backup files or limit the number of files saved. If you specify a number of files to save, then older backups are removed after a scheduled backup is completed and the limit has been reached.

The database is backed up to the specified directory. Saving backups to a separate location such as a network share ensures that an up-to-date copy of the database is available should a problem such as a server disk failure occur. The backup directory must exist and be writable or it will not be accepted. Both the start and stop of the database backup are logged to the Console Event View log for verification and tracking purposes.

The Backup Alarm and Reporting Database checkbox lets you enable and disable the automatic backup of alarm data and Extreme Management Center reporting data. Because the alarm and reporting databases can be quite large,

this allows you to control the amount of disk space used by the database backup operation.

You can customize the date and time formats of backup files by selecting the option that formats the date -- day (DD), month (MM), and year (YYYY) -- according to your personal preference.

For more information, see Tuning Database Backup Storage in Performance Tuning section of the Extreme Management Center Technical Reference.

Data Display Format

Selecting Data Display Format in the left panel of the Options window provides the following view where you can specify your network mask, MAC address separator, MAC address, and auto group delimiter display options. You can also specify how to display devices in the device tree. These settings apply to the current logged-in user.

Network Mask

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*.

MAC Address Separator

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).

Display MAC Addresses by

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.

Auto Group Delimiter

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.

How to display devices in the device tree

Select one of the following options:

- **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).

Date/Time Format

Selecting Date/Time Format in the left panel of the Options window provides the following view where you can customize the date and time formats to your own personal preference. These settings will apply to the current logged-in user.
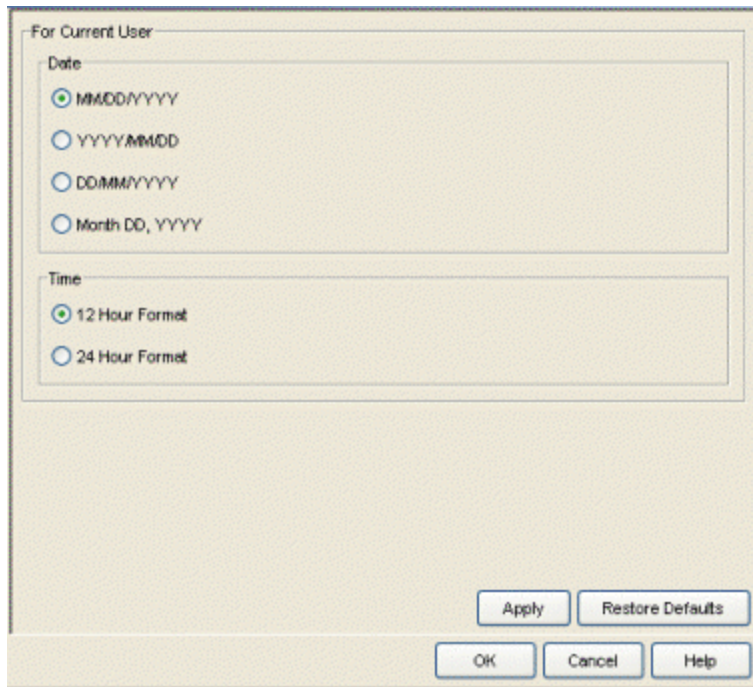
Date

> Select the option that formats the date – day (DD), month (MM), and year (YYYY) – according to your personal preference.

Time

> Select the option that formats the time – 12-hour or 24-hour clock – according to your personal preference.

Diagnostic Configuration

Selecting Diagnostic Configuration in the left panel of the Options window provides the following view where you can configure the level of information collected in client-side diagnostic logs. The information collected in these logs can be used for troubleshooting purposes. Each Extreme Management Center 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 Extreme Management Center applications and various Extreme Management Center components, and lets you configure the level of information to be collected for each one. Select the desired applications and/or components and use the Table Editor to set the level of diagnostic information to collect.
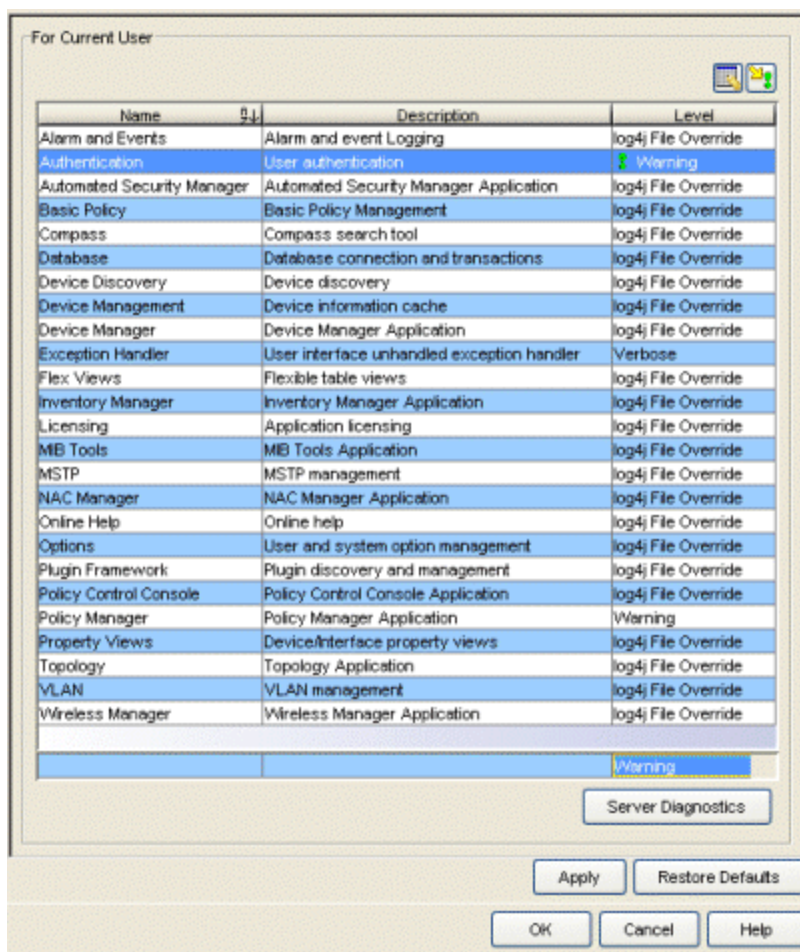
Name and Description

> The name of the Extreme Management Center application or component and a brief description.

Level

The level of information that will be collected in the logs for the selected Extreme Management Center applications and/or components. Use the Table Editor to change the level. Select the row(s) you would like to edit, and toggle the Show/Hide Table Editor button ![icon] 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.

Once you have selected a new level, a green exclamation mark (![icon]) marks the cells that have been changed (but not Applied) and the ![icon] **Apply** button becomes active. Click **Apply** ![icon] to apply the changes to the table.

![icon] **Show/Hide Table Editor**

This button toggles the Table Editor, a row at the bottom of the table that allows you to select the desired level for selected log. Click on the last column in the editor row and use the drop-down list to select the desired level. Click **Apply** ![icon] to apply the changes to the table.

![icon] **Apply**

Click this button to apply changes you have made using the Table Editor.

Server Diagnostics

Opens the Administration web page where you can select the Server Diagnostics tab and specify diagnostic configuration levels for server-side diagnostics.

ExtremeNetworks.com Update

Selecting ExtremeNetworks.com Update in the left panel of the Options window 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.

Schedule Updates

This section lets you schedule a specific times to check for Extreme Management Center software updates. Use the drop-down list to set the frequency (**Daily**, **Weekly**, **Disabled**) for checking for updates. If you have specified 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 have specified a Daily update, set the desired time.

Extreme Access Control Assessment Web Update Server
> Displays the web update server used by NAC Manager 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, click the **Edit** button 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 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.

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 user name and password for the account, then enter the same credentials here.

MAC OUI Vendor List

Selecting MAC OUI Vendor List in the left panel of the Options window displays the IEEE OUI and Company_id Assignments public mapping list, and lets you update and modify the list. 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.

Use these buttons to add, edit, or delete MAC OUI vendors, or update the MAC OUI Vendor list from either the IEEE website or a file.

MAC OUI

The portion of the MAC address that identifies the vendor.

Vendor

The vendor associated with the MAC OUI.

User Defined

Indicates whether this MAC OUI was added by a NAC Manager user.

Name Resolution

Selecting Name Resolution in the left panel of the Options window displays options related to host name and port name resolution.

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.

Use short hostnames for local addresses

This option is enabled by default when hostname resolution is enabled, and applies to Extreme Management Center 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.

Local address domains

Use the Add Domain field to create a list of *home domains* that will be deleted from a local hostname when it is added to the hostname cache. You can add multiple home domains when subdomains are defined for your network. This option applies to Extreme Management Center only.

The first time the hostname cache service is started, if the Local address domains list has not been defined, Extreme Management Center attempts to auto-populate it by resolving the IP address of the Extreme Management Center server. If it resolves to a subdomain, Extreme Management Center creates multiple entries for all subdomains but the root domain (.com). If it cannot do this successfully, the list will not be populated.

Maximum number of cached resolutions:

The maximum number of IP/hostname pairs that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum number of pending resolutions:

The maximum number of hostname resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Aging threshold (hours):

This option determines how long IP/hostname pairs will be cached in memory. After the aging threshold time has passed, the IP/hostname pair is removed from the cache in order to prevent stale IP-hostname associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, hostnames will continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

DNS Lookups Per Minute:

The maximum number of hostname lookups that the DNS server can perform each minute. This prevents hostname resolution from using so many resources on a switch that switching of real traffic is affected.

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.

Maximum number of 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 number of 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.

Interface name change polling interval:
> This setting specifies how often the port name resolution service checks devices to see if port information has changed.

Advanced Setting
> Click the Advanced Settings button to open the Name Resolution Advanced Settings Options window.

Extreme Management Center Feedback Program

This option allows you to enable or disable participation in the Extreme Management Center Customer Feedback Program. If you participate, Extreme Management Center gathers anonymous usage information to better understand how Extreme Management Center 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 Extreme Management Center that automatically upload troubleshooting information, and more.

The information gathered will not be used for marketing purposes or to contact you.

Extreme Management Center Server Health

Selecting Extreme Management Center Server Health in the left panel of the Options window provides the following view, from which you can configure warnings to help monitor the NetSight server health.

Low Memory Threshold (percent)

> Enter a percentage to specify the server heap memory utilization percentage above which an alarm is raised. If the memory utilization falls more than five percent below the threshold percentage, the alarm is automatically cleared.

Send e-mail if the database connection fails

> Select the checkbox and enter an email address to send an email notification if the Extreme Management Center database goes down and when the database comes back up.

Network Monitor Cache

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 Extreme Management Center that request it. The cache should generally be left enabled for the best experience.
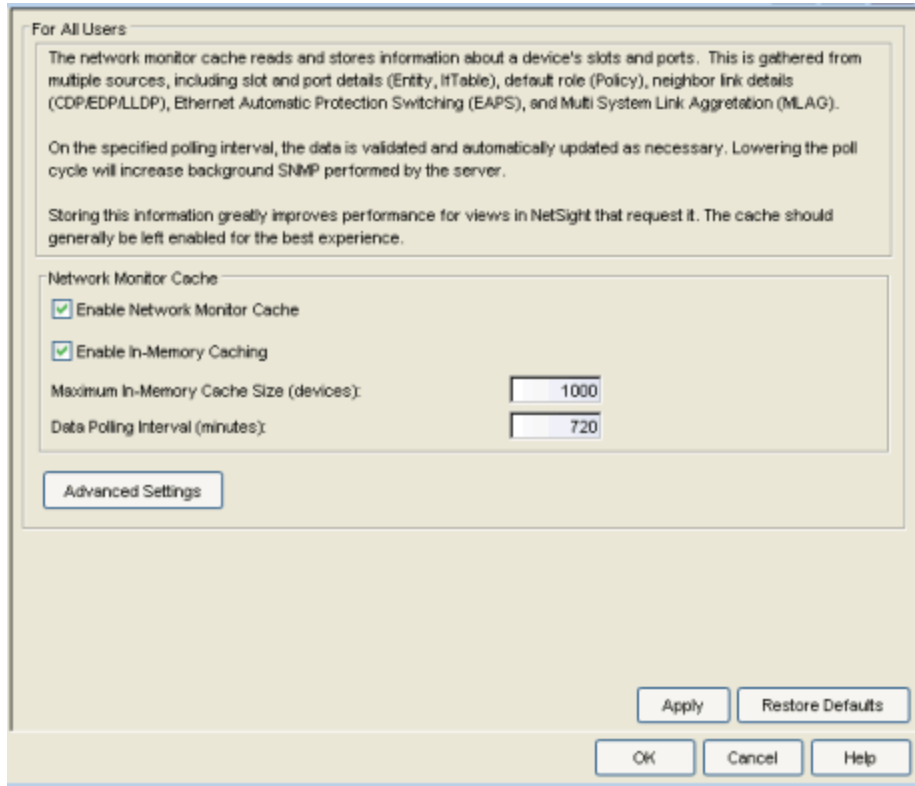
Enable Network Monitor Cache

Use this option to enable or disable the network monitor cache. Enabling the cache improves performance for Extreme Management Center views that request this information.

Enable In-Memory Caching

Use this option to enable or disable the In-Memory Cache. To limit memory usage, you can disable the In-Memory Cache and have the Device Cache rely directly on the database.

Maximum In-Memory Cache Size

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.

Data Polling Interval

The frequency (in minutes) that the device data is checked for changes. If the device data is stale, the data is refreshed in the cache. Reducing the interval will increase background SNMP performed by the server.

Advanced Settings

Opens a window where you can set network monitor cache advanced
options.

- **Maximum number of SNMP worker threads.** The cache is populated with results
  from SNMP queries to devices. If multiple devices are added to the cache at the same
  time, this number determines the maximum number of threads that 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.

Port Monitor

Selecting Port Monitor in the left panel of the Options window provides the
following view where you can specify Port Monitor display options. These
settings will apply to the current logged-in user.

Interval between Polls

The amount of time (in seconds) between polls of the device.

Table Colors

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.

Enable Display of Port Monitor Data

Use the checkboxes in this section to determine 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.

Maximum Open Port Monitor Count

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.

Services for Extreme Management Center Server

Selecting Services for Extreme Management Center Server in the left panel of the Options window provides the following view where you can specify your TFTP settings. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.
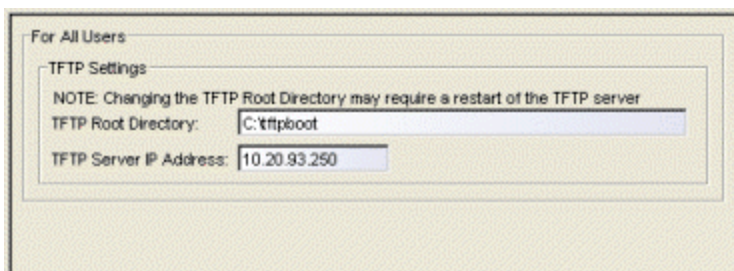
TFTP Root Directory

You must specify a TFTP root directory, whether you are using the Extreme Management Center TFTP server or another TFTP server. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server 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 Extreme Management Center TFTP service,** keep in mind the following requirements when setting the path to your root directory:

- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.

- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive (e.g. C:\ or D:\).

- **If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using `h:\` (where h:\ is mapped to the tftpboot directory on the remote drive)
use
`\\yourservername\tftpboot\`

TFTP Server IP Address

If the TFTP server resides on a remote system, or if the local system is configured with multiple IP addresses, enter the IP address for the TFTP service here. This field accepts both IPv4 and IPv6 addresses.

SMTP E-Mail Server

Selecting SMTP E-Mail Server in the left panel of the Options window provides the following view where you can specify the SMTP E-Mail server that will be used by the Extreme Management Center E-Mail notification feature. The E-Mail notification feature is used in Console's alarm action configuration and in Inventory Manager's Capacity Planning report scheduling. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Outgoing E-Mail (SMTP) Server
>   Identifies the SMTP (E-Mail) server that should be used for outgoing messages generated by the E-Mail notification feature.

Sender's Address
>   The sender's address that is inserted in outgoing E-Mail notification messages. The address should be in a fully qualified format such as "sender's name@sender's domain."

SMTP Password
>   The password that must be entered by the user before the email can be processed.

Show password in clear text
>   When checked, the password is shown in text. When unchecked, the password is shown as a string of asterisks.

Status Polling

Selecting Status Polling in the left panel of the Options window provides the following view where you can 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 Extreme Management Center 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.

SNMP

These status polling options pertain to devices whose poll type is set to "SNMP."

Maximum number of devices to contact at once.
> The maximum number of IP addresses that Console will attempt to contact simultaneously.

Ping

These status polling options pertain to devices whose poll type is set to "Ping."

Number of Ping Retries
> 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.

Length of Ping Timeout (in seconds)
> The amount of time (in seconds) that Console waits before re-trying to ping a device. The default setting is 3 seconds. The maximum setting is 20 seconds.

Maximum number of devices to contact at once.
> The maximum number of IP addresses that Console will attempt to contact simultaneously.

Poll Groups

There are three poll groups that each define a unique poll frequency. The poll frequency for each group specifies the actual length of the poll cycle in seconds. The interval for individual poll groups can be set according to your network's needs using the guideline under Optimal Poll Intervals.

Select one group as the default poll group. 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 Access view in Console's Properties tab.

Events

When this option is selected, only SNMP timeout errors will result in a "Contact Lost" device status. All other SNMP errors will be reported as informational events in the Console Event Log and will not cause the device status to be marked as "down" with a red down arrow.

System Browser

Selecting System Browser in the left panel of the Options window provides the following view where you can specify the web browser for Extreme Management Center to use when launching web pages from Extreme Management Center applications. The browser selections displayed depend on the web browsers installed on your system. Select Default to specify the system default browser. This setting applies to the current logged-in user.
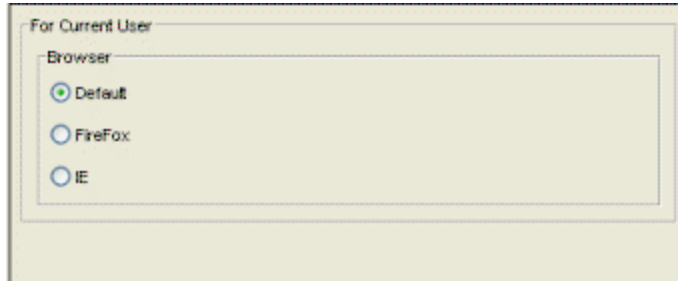
Trap Configuration

Selecting Trap Configuration in the left panel of the Options window provides the following view where you can 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. Clicking Advanced Settings opens the Trap Configuration Advanced Settings window.
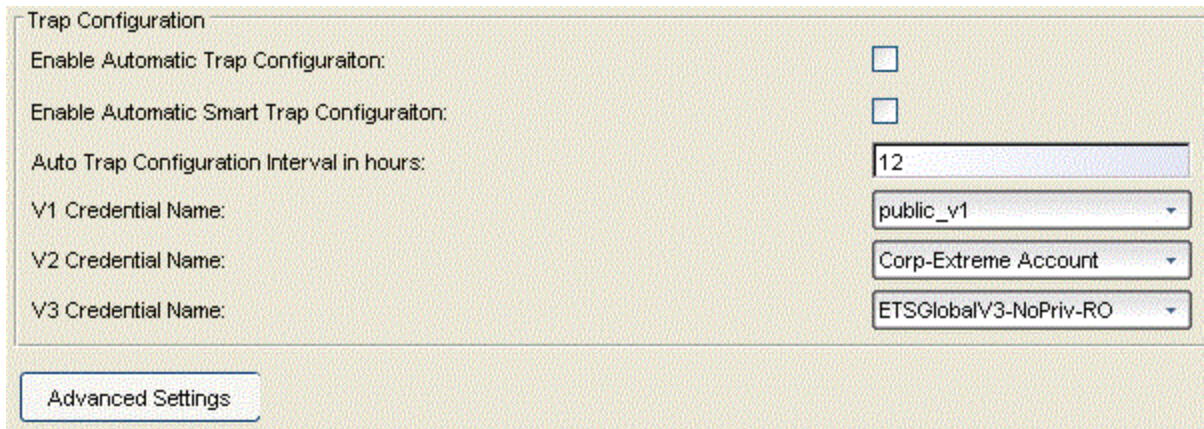
Tree

Selecting Tree in the left panel of the Options window provides the following view where you can 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.

Web Server

Selecting Web Server in the left panel of the Options window provides the following view where you can specify the HTTP and HTTPS port ID for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8080 (HTTP) and 8443 (HTTPS). If you change the port ID, you must restart the Extreme Management Center Server for the change to take effect.

The HTTP Session Timeout option lets you specify a session timeout value for all Extreme Management Center web-based views, such as Extreme Management Center web pages and Console FlexViews.

The Password AutoComplete 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 NAC Manager for the option to take effect.

These settings applies to all users. You must be assigned the appropriate user capability to change this setting.

Related Information

For information on related tasks:

- How to Set Suite Options

Alarm Advanced Settings Window (Legacy)

Use this window to set advanced alarm settings. You can access the window from the Alarm Configuration view in the Suite options (Tools > Options > Suite).
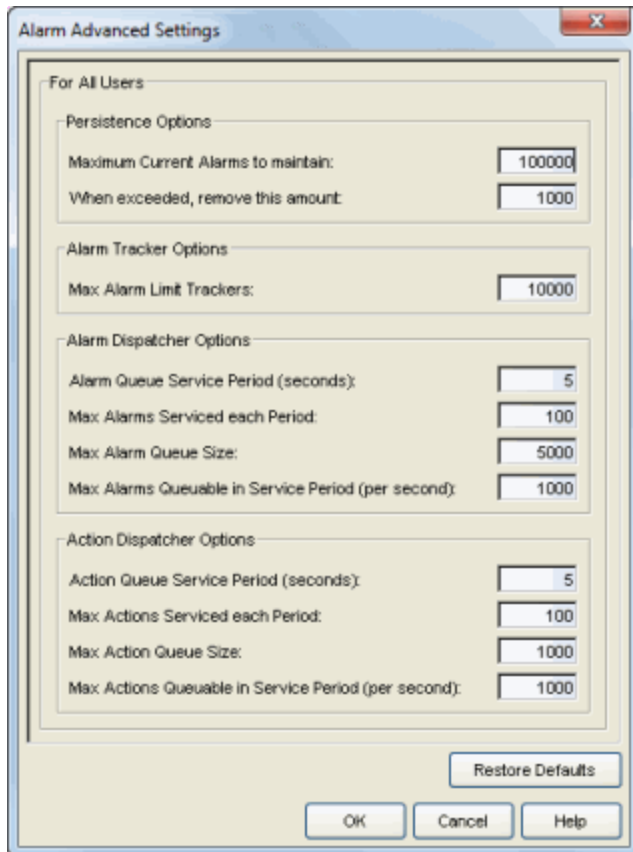
Persistence Options

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, you should be sure the server system can handle the increased load. The number of alarms to remove should be increased only if the maximum current alarms number is being exceeded too frequently.

Alarm Tracker Options

When you define an alarm with a limit, Extreme Management Center has to track 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 is performed for an alarm.)

You can increase the number if you are sure the system can handle the increased load.

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 (seconds)
> 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.

Max Alarms Serviced each 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.

Max Alarm Queue Size
> The maximum number of alarms that can be queued. By default, the dispatcher drops alarms after 5000 alarms are queued.

Max Alarm Queuable in Service Period (per second)
> This limits the rate that 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.

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 (seconds)

> This controls how often the queue is checked for alarms/actions to process. The dispatcher runs once every service period. So by default, the dispatcher processes alarms/actions every 5 seconds.

Max Actions Serviced each Period

> The maximum number of actions pulled from the queue for processing each service period. By default, the dispatcher processes 100 actions every service period.

Max Action Queue Size

> The maximum number of actions that can be queued. By default, the dispatcher drops actions after 1000 actions are queued.

Max Actions Queuable in Service Period (per second)

> This limits the rate that 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.

Related Information

For information on related windows:

- [Alarm Configuration View](#)

Edit Proxy Settings Window (Legacy)

If your network is protected by a firewall, use this window to configure proxy server settings to use when accessing the ExtremeNetworks.com website to obtain update information about Extreme Management Center software releases and Extreme Networks firmware releases available for download. You can access the window from the ExtremeNetworks.com Update view in the Suite options, by clicking the **Edit** button in the HTTP Proxy Server section.

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 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.

Related Information

For information on related windows:

- [ExtremeNetworks.com Update view](#)

Name Resolution Advanced Settings Options Window (Legacy)

Use this window to set advanced name resolution options. You can access the window from the [Name Resolution view](#) in the Suite options.
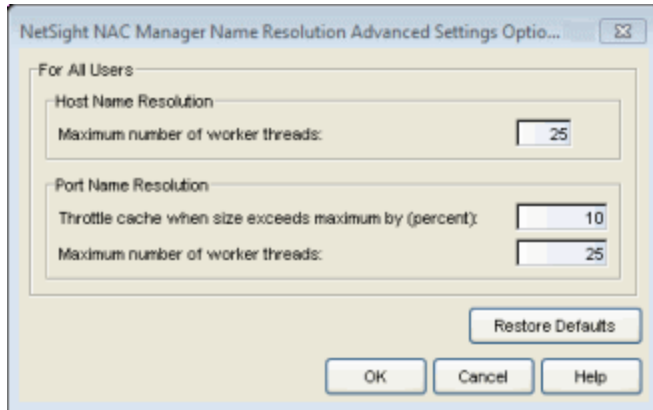
Host Name Resolution

Use this section to set advanced options for host name resolution.

Maximum number of worker threads:

> The maximum number of hostname lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by host name resolution.

Port Name Resolution

Use this section to set advanced options for port name resolution.

Throttle cache when size exceeds maximum by (percent)

> Controls how much port data is discarded from the cache when its size is exceeded. Adjust this to control how an overfull cache is reduced.

Maximum number of 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.

Related Information

For information on related windows:

- [Name Resolution View](#)
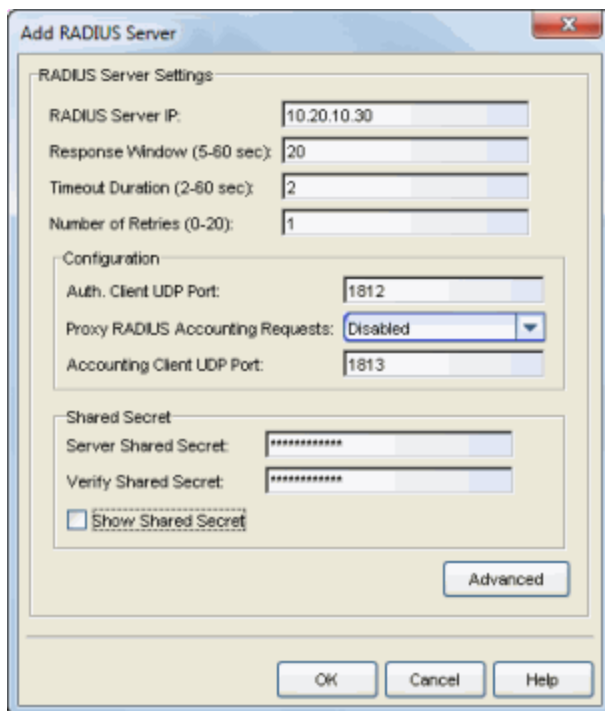
RADIUS Configuration in Extreme Management Center

The Help topics in this section describe how to add, edit, and manage the RADIUS servers used in your Extreme Management Center applications.

Add/Edit RADIUS Server Window

Use the Add/Edit RADIUS Server window to configure the RADIUS servers used in your Extreme Management Center applications. RADIUS servers can be used in Extreme Management Center server authentication configurations and in NAC Manager AAA configurations.

You can access this window from the [Users/Groups tab](#) in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by clicking the drop-down menu in the RADIUS Server field. You can also access this window from the Manage RADIUS Servers window. Any changes made in this window are written immediately to the Extreme Management Center database.

RADIUS Server IP

> The IP address of the RADIUS server.

Response Window

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

Timeout Duration

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

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

Number of Retries

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

Auth. Client UDP Port

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

Proxy RADIUS Accounting Requests

Use this option to enable the Extreme Access Control engine to proxy RADIUS accounting requests to the RADIUS server. This option must be enabled if you are doing RADIUS accounting in an Extreme Access Control environment where the

primary RADIUS server is used for redundancy in a single Extreme Access Control engine configuration (Basic AAA configuration only).

Accounting Client UDP Port

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

Server Shared Secret

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

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Advanced Button

Use this button to open the [Advanced RADIUS Server Configuration window](#), where you can configure advanced RADIUS settings used by NAC Manager when proxying access requests to a backend RADIUS server.

Related Information

For information on related windows:

- [Manage RADIUS Servers Window](#)
- [Advanced RADIUS Server Configuration Window](#)

Advanced RADIUS Server Configuration Window

Use this window to configure advanced RADIUS settings used by NAC when proxying authentication requests to a backend RADIUS server. You can access this window by clicking the **Advanced** button at the bottom of the Add/Edit RADIUS Server window.

Username Format

This field is used by NAC to determine what format to use for the username when proxying a request to the backend RADIUS server. There are two options:

- **Strip Domain Name** (default) - This option removes a domain name from the username when proxying the request. This option should be selected unless the backend RADIUS server requires the domain name to be included.

- **Keep Domain Name** - This option keeps any domain names on the username when proxying the request to the backend RADIUS server. If the backend RADIUS server is a Microsoft IAS or NPS server, this option could cause the RADIUS server to time out if a guest comes onto the network with another domain. In that scenario, if the request is proxied to the backend RADIUS server with the domain name, the server will not respond to the request because it is from an unknown domain. Therefore, if you use this option with a Microsoft IAS or NPS server, an advanced AAA configuration should be used

so that only requests for the desired domain(s) are sent to the backend RADIUS server, and all unknown domains are processed locally so they are rejected.

Require Message-Authenticator

Enable this checkbox if the backend RADIUS server requires a message authenticator to be part of the request. If enabled, NAC adds the message authenticator when proxying the request.

Health Check Section

The options in this section are used by NAC to determine how to check the health of a backend RADIUS server, if that server stops responding to requests.

Use Server-Status Request

When selected, NAC will attempt to use Server-Status RADIUS packets as defined by RFC 5997, to determine if the backend RADIUS server is up.

Use Access Request

When selected, NAC will attempt to use an access request message to determine if the RADIUS server is up. The request will be made using the username and password specified below. The username and password do not need to be valid, since NAC is just looking for is a response and a reject would work just as well. The username/password fields are provided in case you want to prevent rejects from being logged in the backend RADIUS server.

Check Interval

The interval to wait between checks to see if the RADIUS server is up. This is only applicable if the Server-Status request or Access request methods are used.

Number of Answers to Alive

The number of times the RADIUS server must respond before it is marked as alive. This is only applicable if the Server-Status request or Access request methods are used.

Revive Interval

If Server-Status requests and Access requests are not allowed or supported by the RADIUS server, then NAC will wait the amount of time specified here before allowing requests to go to a backend RADIUS server, if it stops responding. This is the least favorable approach and should only be used if there is no other way to detect the health of the backend RADIUS server.

Related Information

For information on related windows:

- [Manage RADIUS Servers Window](#)
- [Add/Edit RADIUS Server Window](#)

Manage RADIUS Servers Window

This window lets you view and define the RADIUS servers used in your Extreme Management Center applications. RADIUS servers can be used in Extreme Management Center server authentication configurations and in NAC Manager AAA configurations.

You can access this window from the [Users/Groups tab](#) in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window. Any changes made in this window are written immediately to the Extreme Management Center database.
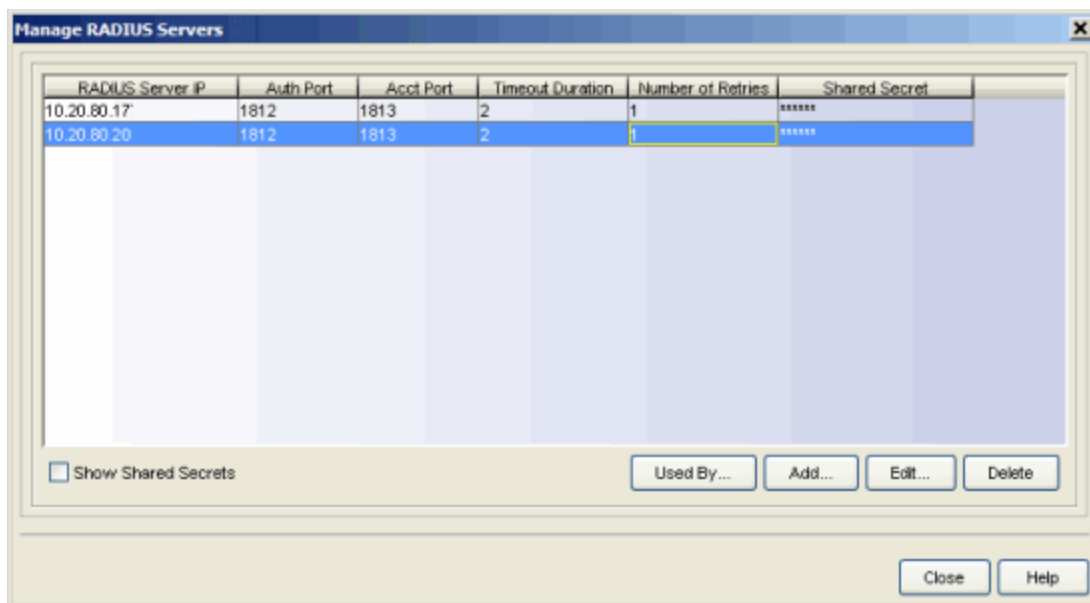
RADIUS Server IP

The IP address of the RADIUS server.

Auth Port

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

Acct Port

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

Timeout Duration

The amount of time in seconds the Extreme Management Center server or Extreme Access Control engine will wait for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds.

Number of Retries

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

Shared Secret

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

Show Shared Secrets

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

Used By Button

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

Add Button

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

Edit Button

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

Delete Button

Deletes the selected RADIUS server. You cannot delete servers that are currently in use.

Related Information

For information on related windows:

- Add/Edit RADIUS Server Window

Server Information

The Server Information tool lets you view and configure certain Extreme Management Center Server functions, including client connections, database properties, database backup and restore, locks, and licenses. It also provides access to a server log and server statistics. You can access this tool from the **Tools > Server Information** menu option in any application.

Server Configuration Considerations

This Help topic provides configuration information for the Extreme Management Center Server, such as limiting client connections to the server, adding memory to the server, firewall considerations, and dealing with SSL vulnerability concerns.

Instructions on:

- Limiting Client Connections on Linux
    - Accepting Connection from Local Client Only
    - Limiting Connections to a Specific IP Address
- Adding Memory to the Server on Linux
- Firewall Considerations
- SSL Vulnerability Concerns

Limiting Client Connections on Linux

Use the steps in this section to configure the server to accept connections only from the local system and/or limit client connections to a specific IP address.

Accepting Connection from Local Client Only

By default, the Extreme Management Center Server accepts connections from any client system. To limit connections to clients connecting from the local system only, use the following steps:

1. Open the server's run.sh file located in
   `<install directory>/jboss/bin/run.sh`.
2. Edit the HOSTNAME variable at the top of the file to:
   `HOSTNAME="127.0.0.1"`

Limiting Connections to a Specific IP Address

By default, the Extreme Management Center Server accepts connections on all IP addresses supported by the server host. If your server supports multiple IP addresses, it may be desirable to limit client connections to a specific IP address. To specify an IP address:

1. Open the server's run.sh file located in
   `<install directory>/jboss/bin/run.sh`.

2. Edit the HOSTNAME variable at the top of the file to:
   `HOSTNAME="<server IP address>"`
   For example, HOSTNAME="123.123.123.123"

Clients must use the exact IP address to connect to the server. Clients can no longer use *localhost*, 127.0.0.1, or any DNS name that translates to anything but the specified IP address.

Adding Memory to the Server on Linux

By default, the Extreme Management Center Server is configured to use a maximum of 512 MB of virtual memory. On large server systems and in large deployments, you can increase the amount of memory. If the server attempts to access more memory than it is configured for, it terminates.

1. Open the server's run.sh file located in
   `<install directory>/jboss/bin/run.sh`.

2. Edit the MAXMEMORY variable at the top of the file to the desired value:
   `MAXMEMORY="<number of MB>"`

Firewall Considerations

- The Extreme Management Center Server runs on a set of non-standard ports. These TCP ports (4530-4533) must be accessible through firewalls for clients to connect to the server.
  4530/4531 -- JNP (JNDI)
  4532 -- JRMP (RMI)
  4533 -- UIL (JMS)

- Port 8080 (Default HTTP traffic) must be accessible through firewalls for users to install and launch Extreme Management Center client applications.

- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Management Center Server Administration web pages, Extreme Management Center, and Extreme Access Control Dashboard.

- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Access Control Engine Administration web pages.

- The following ports must be accessible through firewalls for the Extreme Management Center Server and an Extreme Access Control engine to communicate:
Required Ports (all bi-directionally)
TCP: 4530-4533, 4589, 8080, 8443, 8444
UDP: 161, 162

- The following ports must be accessible through firewalls for the Extreme Management Center Server and Wireless Controllers to communicate:
SSH: 22
SNMP: 161, 162
Langley: 20506

- The following ports must be accessible through firewalls for the Extreme Management Center Server and WAS to communicate:
TCP: Port 8443 - Used by WAS to authenticate Extreme Management Center users. This port corresponds to Extreme Management Center's HTTPs Web Server port.
TCP: Port 443 - Import data from Extreme Management Center into WAS.
TCP: Port 8080 - Upgrade WAS from WAS UI.

- Port 2055 must be accessible through firewalls for the Extreme Management Center Server to receive NetFlow data.

SSL Vulnerability Concerns

The Secure Socket Layer (SSL) protocol allows for secure communication between a web server and a web browser. In Extreme Management Center, it is used to secure communication between the JBoss Web Console server (accessed from the Launch Page Administration tab > Server Utilities tab > JBoss Web Console link) and the web browser client that is accessing it. At the beginning of an SSL session, the server and client negotiate the encryption algorithm, known as a cipher. The chosen cipher is generally the strongest one which is supported by both the server and client. SSL encryption ciphers are classified based on encryption key length as follows:

- HIGH - key length larger than 128 bits

- MEDIUM - key length equal to 128 bits

- LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt and a remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

To increase SSL security, you can disable support for LOW encryption ciphers by adding a line to the nsjboss.properties file that specifies the encryption ciphers used. The line (as it appears below) only lists MEDIUM and HIGH ciphers; all LOW ciphers have been removed. The values are comma delimited and you can customize the list as desired. If this line is not added, then all ciphers will be included.

1. Open the nsjboss.properties file (`<install directory>\appdata\nsjboss.properties`) in a text editor.

2. Cut and paste the following line into the file:
   enterasys.tomcat.ciphers=SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA

3. Save and close the file.

4. Restart the Extreme Management Center Server.

To remove a cipher (for example, if a vulnerability scan lists one of the ciphers as insecure), simply delete the cipher from the list.

1. Open the nsjboss.properties file (`<install directory>\appdata\nsjboss.properties`) in a text editor.

2. Delete the cipher from the list. For example, the cipher SSL_RSA_WITH_RC4_128_MD5 has been removed from the list:
   enterasys.tomcat.ciphers=SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA

3. Save and close the file.

4. Restart the Extreme Management Center Server.

Related Information

For information on related tasks:

- How to Configure and Manage the Extreme Management Center Server
- How to Stop and Start the Extreme Management Center Server

For information on related windows:

- Server Information Window

How to Configure and Manage the Server

Use the Server Information window to manage various Extreme Management Center Server functions including viewing server information, configuring client connection options, and managing the database. To access this window, select **Tools > Server Information** from the menu bar. You must be assigned the appropriate user capability to access this view.

Instructions on:

- Console Client Connections Options
- Managing the Database
    - Changing the Database Password
    - Changing the Database Connection URL
    - Performing a Database Backup
    - Restoring the Initial Database
    - Restoring a Saved Database
- Viewing Client Connections
    - Disconnecting a Client
- Viewing Licenses
    - Changing a License
- Viewing Locks
    - Revoking a Lock
- Viewing the Server Log
- Viewing Server Statistics

Console Client Connections Options

The Client Connections Options window lists the number of current client connections for each installed application, and lets you change the maximum number of connections allowed for each application and the Extreme Management Center Server. You can access this window by clicking the **Configure** button in the Server Information window.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Click the **Configure** button. The Client Connections Options window opens.

3. The number of current client connections for each installed application displays. In the **Total Allowed** column, the maximum number of client connections allowed by this application displays. Select this column and use the arrows to change the number, if desired.

4. Below the table, the **Number of Clients Allowed** field shows the maximum number of concurrent client connections allowed by the Extreme Management Center Server. Use the arrows to change the number, if desired. This number should be set to the total number of clients you want to allow to connect to the server.

5. Click **OK**.

Managing the Database

Use the <u>Database tab</u> in the Server Information window to change the database server password and connection URL, as well as perform database backup, initialize, and restore operations. To access the tab, select **Tools > Server Information** from the menu bar. The Server Information window opens, where you can select the **Database** tab.

Changing the Database Password

Database server properties are used by the Extreme Management Center Server when it connects to the database. The database is secured via a credential comprised of a user name and password. Use the following steps to change the database password.

IMPORTANT: When Console is installed, it automatically secures the MySQL database server by removing all the root and anonymous users from the MySQL user database. Console then adds one generic user name (user = netsight) and password (password = enterasys). Change this password immediately as all customers who install Console know this generic password.

---

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Database** tab.

3. In the Database Server Properties section, select the **Show Password** checkbox to display the password, if desired.

4. Click **Change** to open a window where you can enter a new password. (The password is masked unless you selected the **Show Password** checkbox.) Click **OK**.

5. You must restart both the Extreme Management Center Server and client after you change the database password.

Changing the Database Connection URL

The Connection URL is 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 using the following steps.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Database** tab.

3. In the Database Server Properties section, enter a new URL in the following format:
   `jdbc:mysql://[hostname]/<database>`
   where [*hostname*] is optional. Click **Apply.**

4. You must restart both the Extreme Management Center Server and client after you change the database connection URL.

Performing a Database Backup

You can save the currently active database to a file on the Extreme Management Center Server workstation. If the Extreme Management Center Server is local, you can specify a directory path where you want to store the backup file. If the server is remote, the database saves to the default database backup location.

NOTE: To schedule regular database backups, use the Database Backup option available from Tools > Options > Suite Options > Database Backup.

---

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Database** tab.

3. In the Extreme Management Center Data Set Operations section, click **Backup**. The [Backup Database window](#) opens.

4. The Database Path field displays the default database backup location. If the Extreme Management Center Server is local, you can specify an alternate backup directory by entering a path to the directory, or using the **Browse** button to navigate to the directory. If the server is remote, the database is saved to the default database backup location.

5. In the Database Name field, enter a name for the database backup file.

6. Click **Backup** to begin the database backup operation.

Restoring the Initial Database

Restoring an initial database removes all data elements from the database and populates the Extreme Management Center Administrator authorization group with the name of the logged-in user. This operation causes all current client connections and operations in progress to be terminated.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Database** tab.

3. In the Extreme Management Center Data Set Operations section, click **Restore**. The [Restore Database window](#) opens.

4. Select the **Restore Initial Database** option.

5. Click **Restore** to begin the initialize database operation.

6. You must restart both the Extreme Management Center Server and the client following an initialize database operation.

7. Enforce all Extreme Access Control engines.

Restoring a Saved Database

You can restore a saved database (from a database backup operation) using these steps. This operation causes all current client connections and operations in progress to be terminated.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the Database tab.

3. In the Extreme Management Center Data Set Operations section, click **Restore**. The [Restore Database window](#) opens.

4. Select the **Restore Saved Database** option.

5. Specify the database you wish to restore or use the **Browse** button to navigate to the database. If the server is remote, you only have access to databases in the default database backup directory.

6. Click **Restore** to begin the database restore operation.

> **NOTE:** When restoring a saved 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>\NetSight\services\nsserver.cfg` file needs to be duplicated on the new server when the database is restored. To change the memory setting to match the previous server, stop the 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. For instructions on modifying the my.ini file, see the Change the MySQL my.ini File section in the Extreme Access Control (NAC) Deployment Guide.

7. Enforce the Extreme Access Control engines.

Viewing Client Connections

The Client Connections tab in the Server Information window provides information that lets you view and manage current client connections to this server, and also view a history of client connections. To access the tab, select **Tools > Server Information** from the menu bar. The Server Information window opens, where you can select the Client Connections tab.

Disconnecting a Client

Use the following steps to disconnect a client from the Extreme Management Center Server.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Client Connections** tab.

3. In the Current Client Connections table, select the client that you want to disconnect and click the **Disconnect** button.

4. The client being disconnected receives a message when their connection is 30 seconds from being terminated. Both tables on this tab update automatically when a client connects or disconnects.

Viewing Licenses

The License tab in the Server Information window displays a list of all licensable Extreme Management Center applications and their respective license information. To access the tab, select **Tools > Server Information** from the menu bar. The Server Information window opens, where you can select the **License** tab. It also lists any Extreme Access Control assessment license and Extreme Access Control VM (virtual appliance) license, if applicable. For more information on the Extreme Access Control virtual appliance license, see Extreme Access Control VM license.

You can also use this tab to change a license. Change a license when upgrading from an evaluation copy to a purchased copy, or upgrading to a license that supports more users/devices.

Contact your Extreme Networks Representative to purchase the software and receive a Licensed Product Entitlement ID that allows you to generate a product license. Prior to changing a license, you must redeem your Entitlement ID for the new product license. Refer to the instructions included with the Entitlement that was sent to you. (For more information, view the Product Licensing information at http://www.extremenetworks.com/support/enterasys-support/how-to/ .)

Changing a License

Use the following steps to change a license when upgrading from an evaluation copy to a purchased copy, or upgrading to a license that supports more users/devices.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **License** tab.

3. Select the license that you want to change and click **Change License**. The Change License window opens.

4. Read and accept the terms of the license agreement and click **OK**.

5. Enter the license text that you received when you generated the product license. (When you purchased your Extreme Management Center software product, you received a License Entitlement ID that allows you to generate a product license. Refer to the instructions included with the License Entitlement ID that was sent to you.)

6. Click **Update**. The license file is updated with the new license text.

Viewing Locks

The Locks tab in the Server Information window lets you view a list of currently held operational locks. To access the tab, select **Tools > Server Information** from the menu bar. The Server Information window opens, where you can select the **Locks** tab.

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 software download.

- to lock a certain function so that only one user can access it at a time. For example, only one user can have the Authorization/Device Access window open at a time.

The Locks tab provides information about each lock, such as who owns the lock, the duration of the lock, and a description of the lock. You can also cancel (revoke) a lock in this tab.

Revoking a Lock

Use the following steps to revoke a lock.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Select the **Locks** tab.

3. In the Current Locks table, select the lock you want to cancel and click **Revoke**.

4. 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.

Viewing the Server Log

Use the Server Log tab in the Server Information window to view a log displaying all the events for the server. To access the tab, select **Tools > Server Information** from the menu bar. The Server Information window opens, where you can select the **Server Log** tab.

A new Server Log is created every day. If the Extreme Management Center Server is local, you can view previous logs using the File tab. The Server Log opens with the log's location and filename displayed in the title bar. Use the Find tab or Filter tab to perform find and filter operations on Server Log entries, and target specific entries of interest. Server Log entries are listed by date and time, with newer entries listed at the bottom.

Viewing Server Statistics

Use the Server Statistics window to view Extreme Management Center Server statistics such as CPU usage. You can also launch Advanced statistics that are useful for troubleshooting purposes.

1. Select **Tools > Server Information** from the menu bar. The Server Information window opens.

2. Click the **Server Stats** button. The Extreme Management Center Server Statistics window opens.

3. Click the **Advanced** button to open the Advanced Statistics window. You must use the **Refresh** button to display current statistical information in this window.

Related Information

For information on related windows:

- Server Information Window
- Backup Database Window
- Restore Database Window
- Console Client Connections Options
- Extreme Management Center Server Statistics Window
- Advanced Statistics Window

How to Stop and Start the Server

This Help topic provides steps for manually stopping and starting the Extreme Management Center server components (Extreme Management Center Database and Extreme Management Center Server).

Instructions on:

- Linux
- Windows

Linux

The Extreme Management Center Server components can be controlled using their own stop and start scripts:

<installdir>/scripts/stopserver.sh

<installdir>/scripts/startserver.sh

Windows

You can manually stop and start the Extreme Management Center Server components from the Extreme Management Center Services Manager on the server system.

1. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar).

2. Right-click the Services Manager icon ▣. (If you don't see the icon, you can start the Services Manager from the **Start > Programs** or **All Programs** menu; select **Startup > Extreme Management Center (NetSight) Services Manager**.)

3. Select the appropriate **Extreme Management Center Server** menu option.

   - **Stop Server and Database** - Stops both the Extreme Management Center Server and Database.

   - **Stop Server** - Stops only the Extreme Management Center Server.

- **Restart Server** - Stops the server and then starts it up again immediately, or just starts the server if the server is already stopped. If the Extreme Management Center Database is not running, it is also started.

The color of the arrow on the Extreme Management Center Services Manager icon indicates the state of the Extreme Management Center Server and Database:

- -- A green arrow indicates the Extreme Management Center Server and Database are running.

- -- A yellow arrow indicates the Extreme Management Center Database is running but the Server is down.

- -- A red arrow indicates the Extreme Management Center Server and Database are both down.

- -- An orange arrow indicates the Extreme Management Center Server is running but the Database is down. This is an error condition and requires that you restart both the Extreme Management Center Server and Database.

Related Information

For information on related tasks:

- [How to Configure and Manage the Extreme Management Center Server](#)
- [Extreme Management Center Server Configuration Considerations](#)

For information on related windows:

- [Server Information Window](#)

How to Update the Server Certificate

This Help topic describes how to replace the Extreme Management Center server certificate. During installation, Extreme Management Center generates a new, unique private server key and server certificate. While these provide secure communication, there may be cases where you 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. Additionally, you may want to 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. If you do not have these, this topic also includes procedures used to generate them.

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

You need the RSA or DSA server private key (in PKCS #8 format) used to generate the server certificate. For "browser-friendly" certificates, the server certificate should identify the Extreme Management Center server by its fully qualified host name. If you do not have the server private key and server certificate, refer to the [instructions for generating](#) them.

If your certificate authority (CA) provides additional intermediate certificates, you need to provide those as well. The intermediate certificates can be used in whatever format the CA provides them. They may be in individual files, in a bundle file, or even in the same file as the server certificate.

NOTE: if you need to convert your key file to a PKCS #8 format, use the following OpenSSL command where <server.key> is the original non-PKCS #8 formatted key file. (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 that you have a replacement server private key and server certificate ready to use. If you do not, refer to the Generating a Server Private Key and Server Certificate section below.

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 Server Information window from any Extreme Management Center application (Tools > Server Information). Click on the Certificates tab.

2. Click the **Update Server Certificate** button. The Update Server Certificate window opens.

3. Select the option to provision a private key and certificate from files.

4. In the Private Key section, provide a file containing the private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field.

5. In the Certificate Files section, use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

6. Click **OK**. You will see a confirmation window listing your file information so that you can confirm that the information you have provided is correct. Click **Yes** to proceed with the certificate replacement. The private key and server certificate are updated on the Extreme Management Center server.

7. Restart the Extreme Management Center server to deploy the new private key and server certificate. For instructions on how to restart the server, see How to Stop and Start the Extreme Management Center Server.

Verifying the Certificate

Once the new server certificate is installed and the server has restarted, use one of the following methods to verify that 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`. If your intention was to eliminate browser warnings, verify that no browser warnings are displayed when you access the web page.

2. Then, 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. You need to terminate the program with CTRL-C.

Generating a Server Private Key and Server Certificate

If you do not have a server private key and server certificate to use as a replacement, you can generate them using the instructions in the sections below. You need to:

1. Generate a server private key. It is recommended that you use OpenSSL to generate an RSA key.

2. Create a Certificate Signing Request.

3. Submit the request to a Certificate Authority or generate a self-signed certificate.

4. Verify the contents of the server certificate.

You can use the following steps regardless of whether you are using a commercial certificate authority or an in-house certificate authority.

Generate a Server Private Key

Use the following steps to generate an encrypted RSA private key.

1. 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
```

2. 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.

Create a Certificate Signing Request

Use the following steps to create a Certificate Signing Request (CSR).

1. 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
   ```

2. 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
   ```

Submit the Request to a Certificate Authority

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.

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
```

Advanced Statistics Window

This window provides advanced server statistics that are useful as a troubleshooting tool. You can access this window by clicking the **Advanced** button in the [Server Statistics window](#).

Statistics are provided on the following server functionality. In each tab, you must use the **Refresh** button to display current statistical information.

- Server Status
- Device Status Poller
- Messaging
- Database Status
- NetSightMBean Status
- EventsAndAlarmsMBean Status

You may find it useful to copy information from these tabs and paste it elsewhere. For example, you may want to include the information in an e-mail. However, the text in some of these tabs is in .html format. On Windows platforms you should copy and paste the text into a word processing program that preserves .html format, such as Microsoft Word. (Microsoft Notepad and WordPad do not preserve the .html format.) On Linux and Solaris platforms you can do a Ctrl-c to copy the text and insert it into vi, however the formatting is not preserved.

The Server Status Tab in the Advanced Statistics Window
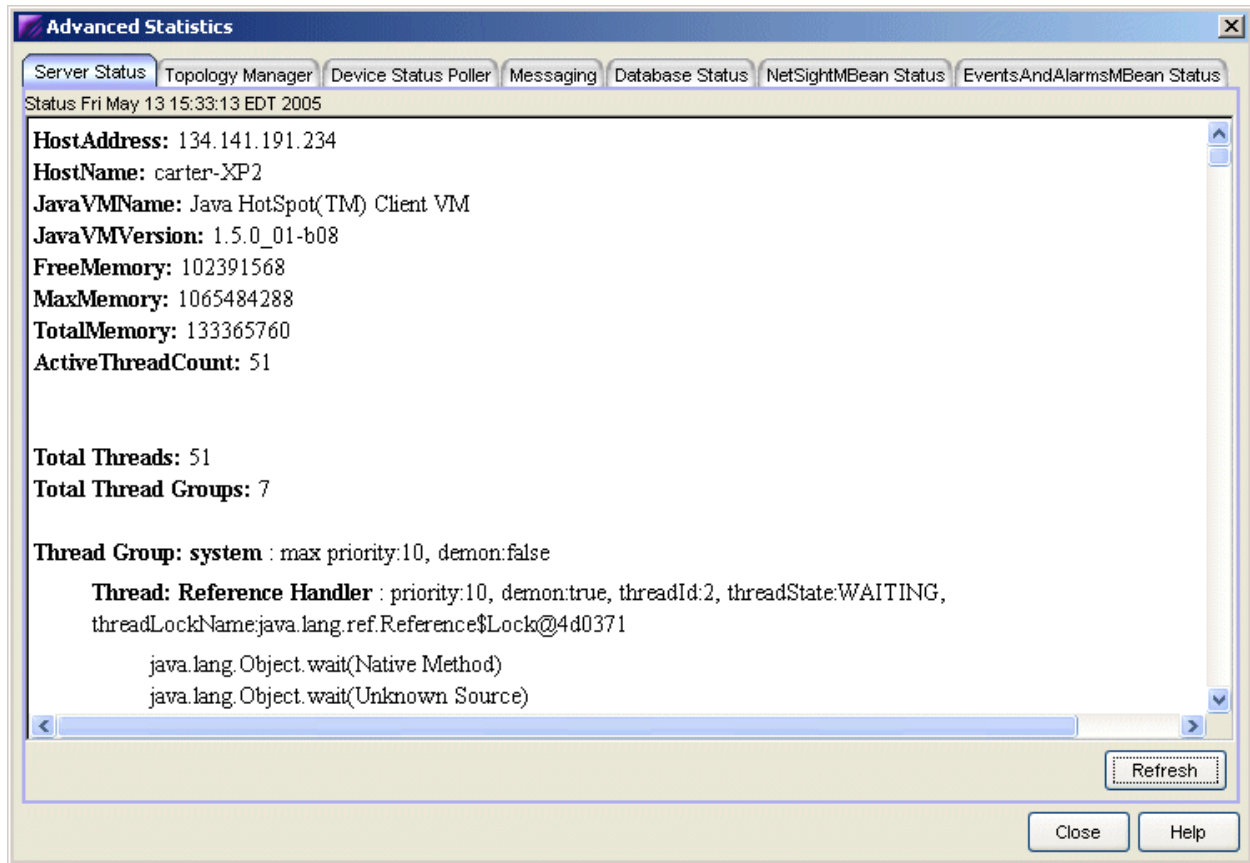
Related Information

For information on related windows:

- Server Information Window
- Server Statistics Window

Backup Database Window (Legacy)

Use the Backup Database window to save the currently active database to a file on the Extreme Management Center Server workstation. If the Extreme Management Center Server is local, you can specify a directory path where you would like the backup file stored. If the server is remote, the database is saved to the default database backup location. You can access this window by clicking the **Backup** button in the [Database tab](#) of the Server Information window.

> **NOTE:** To schedule regular database backups, use the Database Backup option available from Tools > Options > Suite Options > Database Backup.
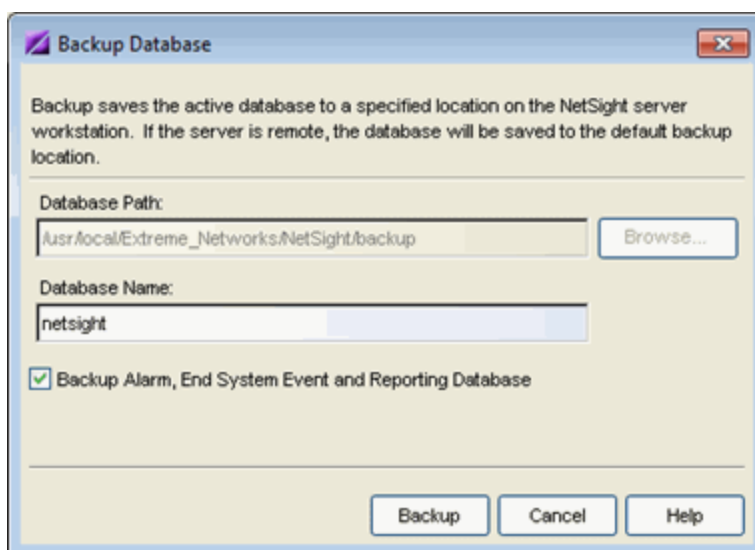
Database Path
> The default database backup location. If the Extreme Management Center Server is local, you can specify an alternate backup directory by entering a path to the directory, or using the **Browse** button to navigate to the directory. If the server is remote, the database is saved to the default database backup location.

Database Name
> Enter a name for the database backup file.

Backup Alarm, End System Event and Reporting Database
> The Backup Alarm, End System Event and Reporting Database checkbox lets you enable and disable backup of alarm, end-system event and reporting data as part of

the backup operation. Because the database can be quite large, this allows you to control the amount of disk space used by the database backup operation.

Backup Button

Starts the backup operation.

Related Information

For information on related windows:

- Server Information Window

Console Client Connections Options

The Console Client Connections Options window lets you see the number of current client connections for each installed application, and change the maximum number of connections allowed for each application and the Extreme Management Center Server. You can access this window by clicking the **Configure** button in the Server Information window. You must be assigned the appropriate user capabilities to access and use this window.
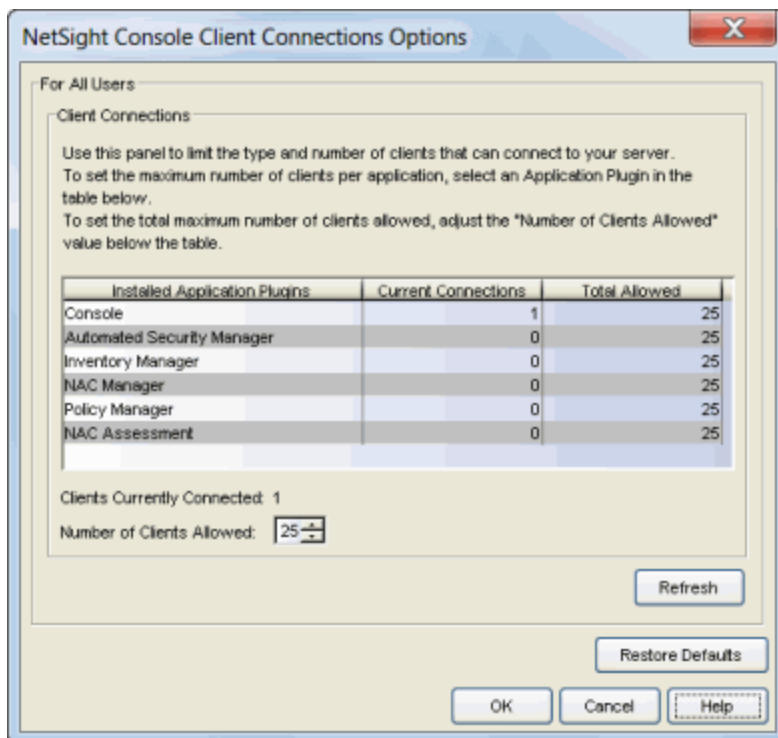
Installed Application Plugins

> The name of the installed application with clients connecting to the Extreme Management Center Server.

Current Connections

> The number of current client connections for this application.

Total Allowed

> The maximum number of client connections allowed for this application. Select this field and use the arrows to change the number, if desired.

Clients Currently Connected

The total number of clients currently connected to the Extreme Management Center Server.

Number of Clients Allowed

The maximum number of concurrent client connections allowed by the Extreme Management Center Server. Use the arrows to change the number, if desired. This number should be set to the total number of clients you want to allow to connect to your server.

Refresh

Refreshes the current connection information.

Related Information

For information on related windows:

- [Server Information Window](#)

Restore Database Window (Legacy)

Use the Restore Database window to restore the initial database or restore a saved database. Both functions cause all current client connections and operations in progress to be terminated. You can access this window by clicking the **Restore** button in the [Database tab](#) of the Server Information window.

> **IMPORTANT:** After restoring the Extreme Management Center server, enforce all Extreme Access Controlengines.
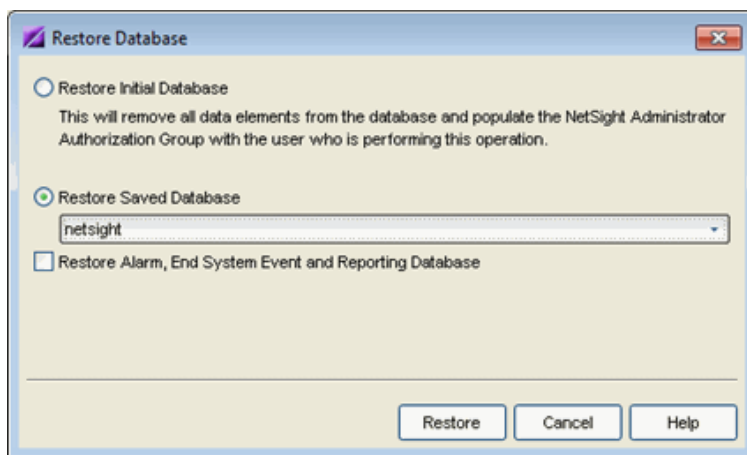
Restore Initial Database

Restoring an initial database removes all data elements from the database and populates the Extreme Management Center Administrator authorization group with the name of the logged-in user. You must restart both the Extreme Management Center Server and the client following an initialize database operation.

Restore Saved Database

Specify the database you wish to restore or use the **Browse** button to navigate to the database. If the server is remote, you only have access to databases in the default database backup directory.

NOTE: When restoring a saved database to a new 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. For instructions on modifying the my.ini file, see the Change the MySQL my.ini File section in the Extreme Access Control (NAC) Deployment Guide.

Restore Alarm, End System Event and Reporting Database

The **Restore Alarm, End System Event and Reporting Database** checkbox lets you enable and disable restoring alarm, end-system event and reporting data as part of the restore operation. This option is only enabled if you have selected the Restore Saved Database option and the selected backup has a Extreme Management Center database included with it.

Restore Button

Starts the restore operation.

Related Information

For information on related windows:

- Server Information Window

Server Information Window

The Server Information window lets you view and configure certain Extreme Management Center Server functions, including management of client connections, database backup and restore, locks, and licenses. It also provides access to the server log and server statistics. To access this window, select **Tools > Server Information** from the menu bar. You must be assigned the appropriate user capabilities to access and use this window.

Click the link for information on the following Server Information window tabs:

- Client Connections
- Database
- Locks
- Server Log
- License
- Certificates

Client Connections Tab

The Client Connections tab provides information that lets you view and manage current client connections to this server, and also view a history of client connections.

Current Client Connections

This 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.

Show System Connections

Check this checkbox to display system connections in addition to standard client connection. System connections include connections for several web services as well as connections that are opened for the Extreme Management Center Scheduler report PDF generation.

Disconnect 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.

Client Connection Log

The client connection log displays a list of all client connect and disconnect activities, and allows you to track the history of a particular client connection. The table displays the last 50,000 log entries, and updates automatically when a client connects or disconnects. The current log file is automatically archived when its size reaches 1 megabyte and opens a new log.

Acknowledge

This checkbox lets you acknowledge an event and also hide items that have been acknowledged. Click the checkbox to acknowledge the item and then click the Show Acknowledged Events button to hide or show the checked items.

Severity

The event's severity.

Category

The category of event: user connection.

Timestamp

The date and time when the event occurred.

Client

The name of the client host machine that triggered the event.

User

The name of the user that triggered the event.

Type

The type of information: event.

Event

> The type of event.

Information

> Information about the client authentication or disconnect.

Show/Hide Acknowledged Events

> This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

Refresh

> Refreshes the log.

Clear Log

> Clears the log. If you want to retain a copy of the log that you are clearing, you must manually copy the date-stamped file in the
> `<install directory>\appdata\logs\admin.log.`

Database Tab

This tab allows you to manage the password and connection URL for the database, and perform database backup and restore operations. You must be assigned the appropriate user capabilities to perform these functions.

IMPORTANT: When Console is installed, it automatically secures the MySQL database server by removing all the root and anonymous users from the MySQL user database. Console then adds one generic user name (user = netsight) and password (password = enterasys). It is recommended that you change this password, since all customers who install Console will know this generic password.
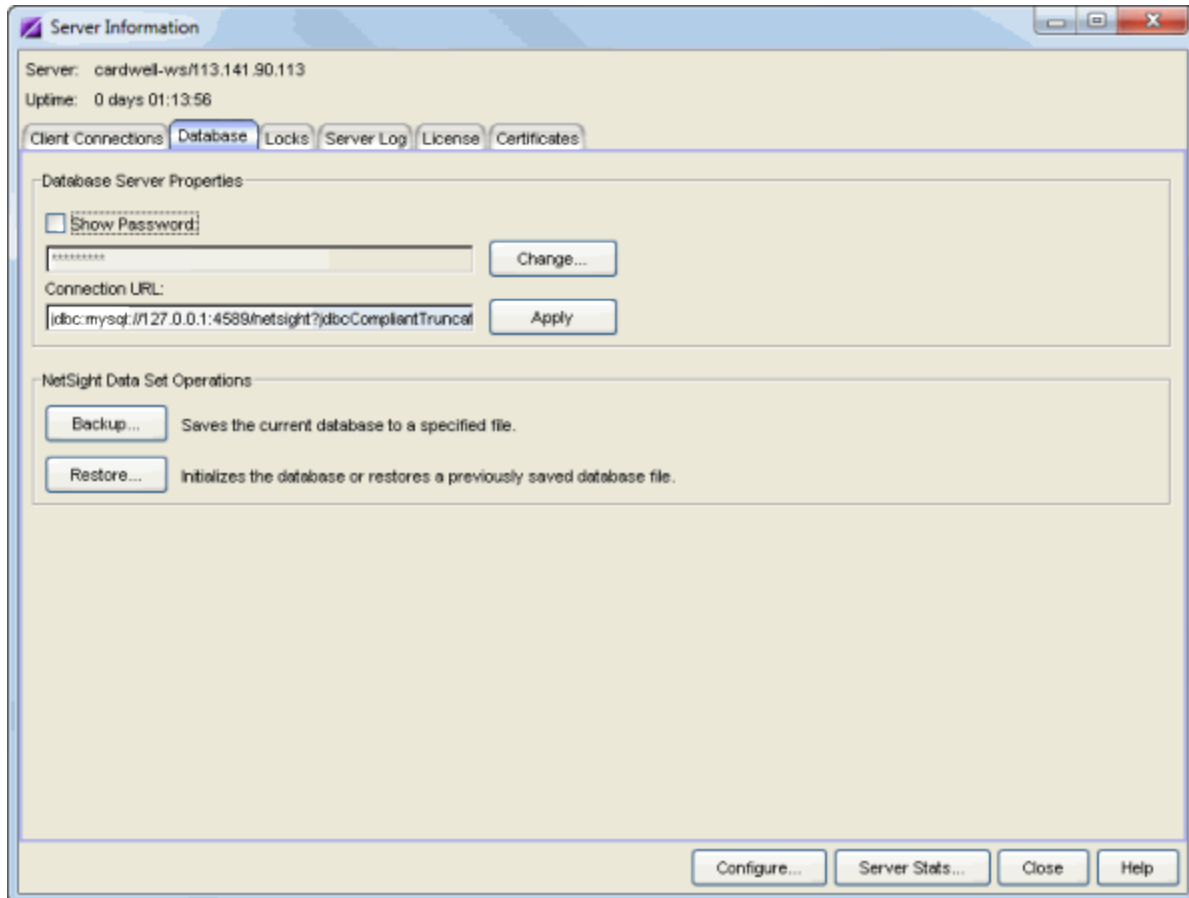
Database Server Properties

Database server properties are used by the Extreme Management Center Server when it connects to the database. The database is secured via a credential comprised of a user name and password (see the Important note above). This area lets you modify that password, and also view and modify the connection URL for the database.

Password

Click **Change** to display a window where you can enter a new password. The password is masked unless you select the checkbox to **Show Password**. You must restart both the Extreme Management Center Server and client after you change the database 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.

You must restart both the Extreme Management Center Server and client after you change the Connection URL.

Extreme Management Center Data Set Operations

This area lets you perform database backup and restore operations.

Backup Button

Opens the Backup Database window where you can save the currently active database to a file. If the Extreme Management Center Server is local, you can specify a directory path where you would like the backup file stored. If the server is remote, the database will be saved to the default database backup location.

Restore Button

Opens the Restore Database window where you can restore the initial database or restore a saved database. Restoring an initial database removes all data elements from the database and populates the Extreme Management Center Administrator authorization group with the name of the logged-in user. Both functions cause all current client connections and operations in progress to be terminated. You must restart both the Extreme Management Center Server and the client following an initialize database operation. When restoring a database, if the server is remote, you only have access to databases in the default database backup directory.

NOTE: When restoring a saved database to a new 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 will need to be duplicated on the new server when the database is restored. To change the memory setting to match the previous server, stop the Extreme Management Center server and edit the nsserver.cfg file.

- The mySQL my.ini file also needs to be manually updated to match any changes made on the original server. For instructions on modifying the my.ini file, see the Change the MySQL my.ini File section in the Extreme Access Control (NAC) Deployment Guide.

Locks Tab

The Locks tab 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 have the Authorization/Device Access window open 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 has been terminated. When the user acknowledges the message, the function closes. You must be assigned the appropriate user capability to revoke a lock.
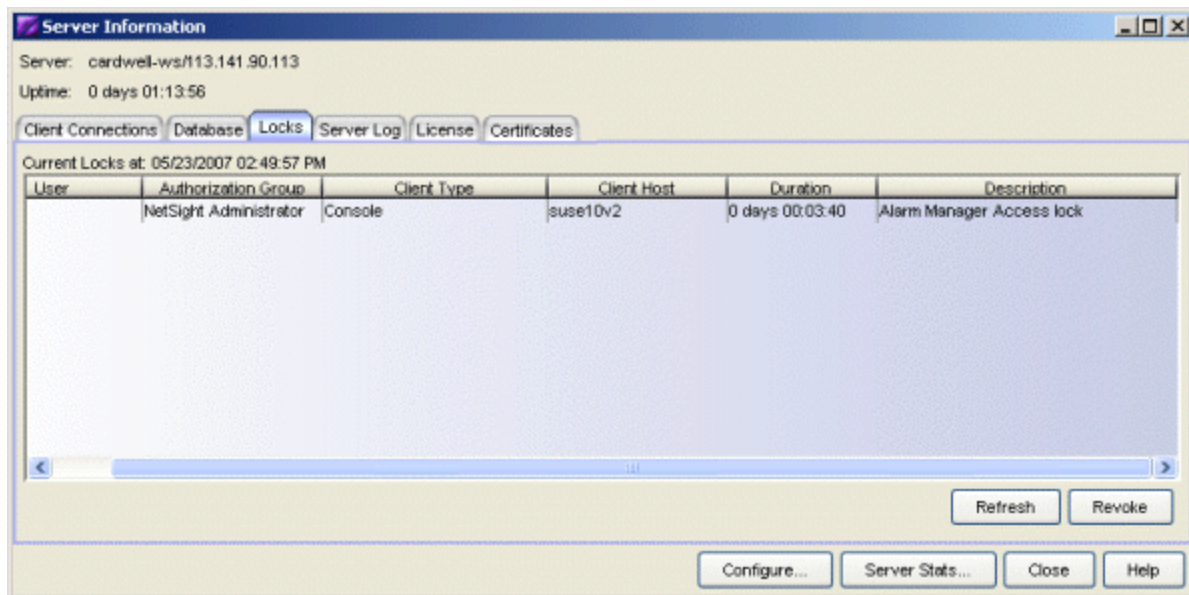
User

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

Refreshes the table and obtains updated lock information.

Revoke Button

Removes the selected lock. When a lock is revoked, a message is displayed on the user's machine informing them that their use of the locked functionality has been terminated. When the user acknowledges the message, the function closes.

Server Log Tab

The Server Log displays all the events for the server. Server Log entries are listed by date and time, with newer entries listed at the bottom. A new Server Log is created every day. If the Extreme Management Center Server is local, you can view previous logs using the File tab.

You can perform Find and Filter operations on Server Log entries to target specific entries of interest. The last Filter and Find settings you enter remain in the Server Log display until you refresh the display.

Information on the following tabs:

- Find Tab
- Filter Tab
- File Tab

Find Tab

The Find tab lets you search the Server Log (filtered or unfiltered) for a specific set of characters, like a word, phrase, or number. Enter your search criteria in the Find field, and when you click the **Find** button, any search terms found will be highlighted in the Server Log display. You can search forward or backward from

your current position, and restrict your search to match the exact upper or lowercase, and/or whole word.
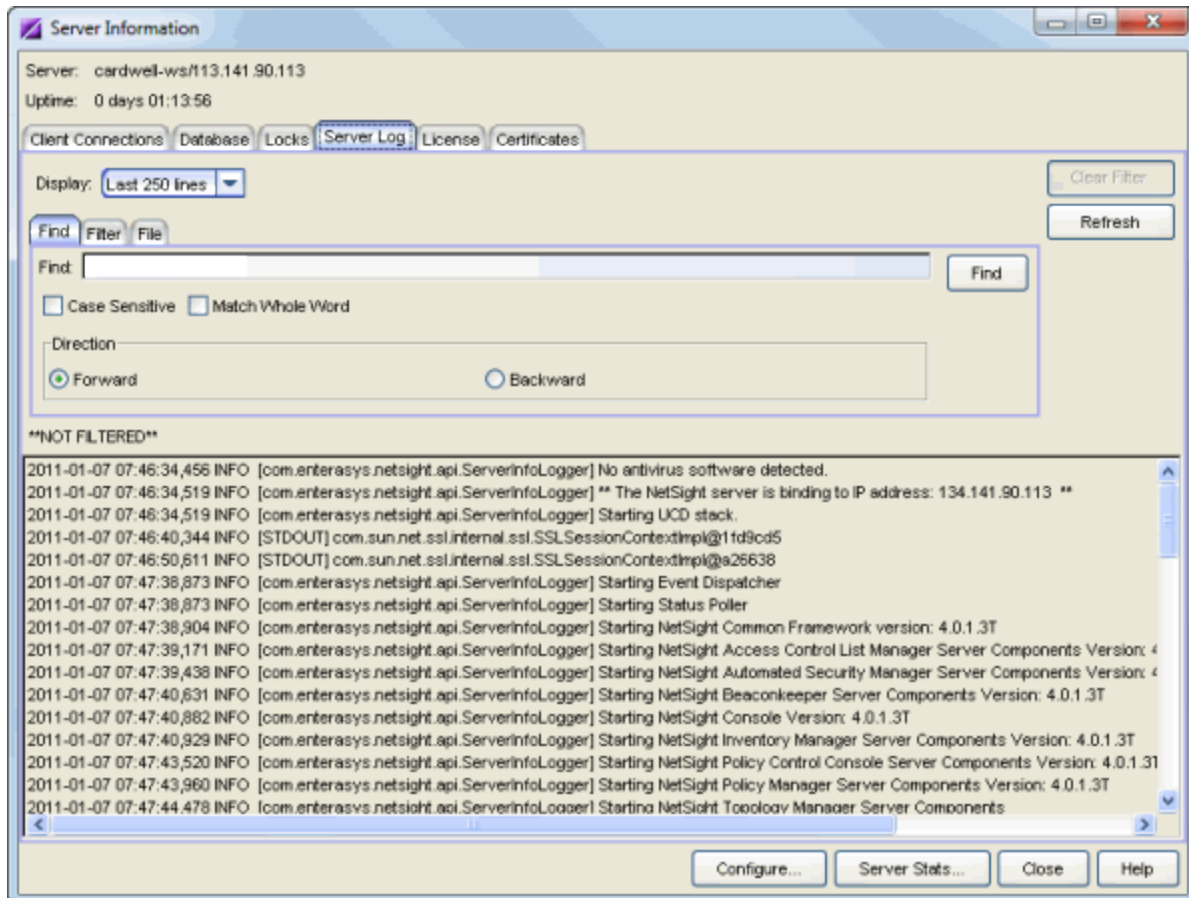
Display:

Use the drop-down list to select the number of lines you would like displayed in the log.

Find:

Enter the text or numeric value you want to find.

Case Sensitive

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Find** field.

Match Whole Word

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Find** field.

Forward

Select **Forward** to search from your current position to the end of the Server Log.

Backward

Select **Backward** to search from your current position to the beginning of the Server Log.

Server Log Entries

Lists the events by date and time, with the more recent entries at the bottom. Directly above the entries you can see the status of whether the entries are filtered or not filtered. Any search terms found are highlighted.

Find Button

Performs the Find operation on the information currently displayed in the Server Log.

Clear Filter Button

Removes any filters currently in effect.

Refresh Button

Displays and updates log entries, and removes any filters. The Server Log does not refresh automatically. If the Server Log is open and new entries are written to the log, you must click **Refresh** to update the log.

Filter Tab

The Filter tab lets you specify which entries to display in the Server Log. Enter the information you want to see, and only matching log entries will be displayed. You can use any combination of filter options, and you can perform consecutive filters on the filtered events.
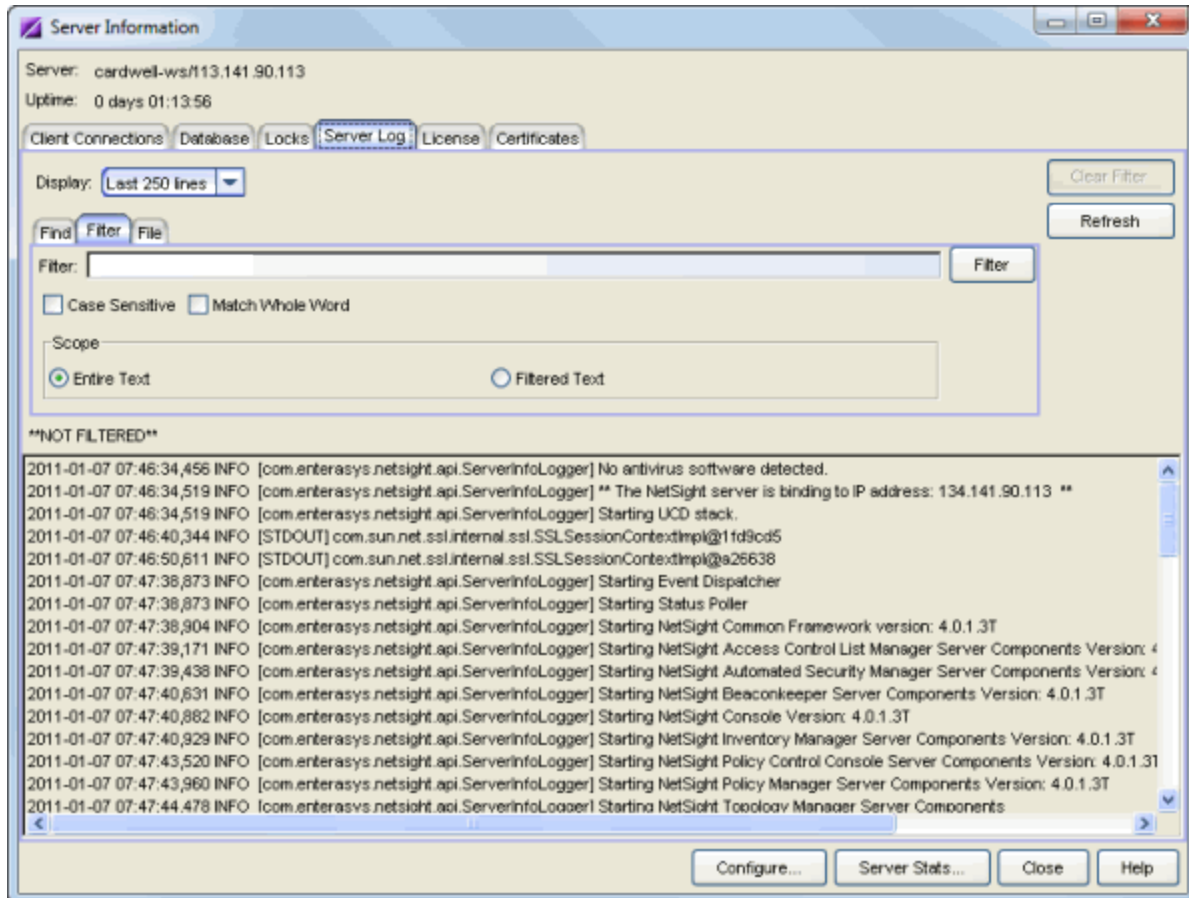
Display:

Use the drop-down list to select the number of lines you would like displayed in the log.

Filter:

Enter the text or numeric value you want to use as a filter.

Case Sensitive

Select this checkbox to search based on an exact match of the upper or lowercase of the text entered in the **Filter** field.

Match Whole Word

Select this checkbox to search based on an exact match of the whole word or numeric value entered in the **Filter** field.

Entire Text

Select the **Entire Text** scope option to filter **all** text by the value in the **Filter** field. If you have already performed a filter, this will enable you to perform a new filter on all entries instead of just the filtered entries.

Filtered Text

> Select the **Filtered Text** scope option to perform a new filter on the results of the previous filter.

Server Log Entries

> After running the filter, this area displays the matching Server Log entries by date and time, with the more recent entries at the bottom. Click **Clear Filter** to remove the filter currently in effect. Directly above the entries you can see the status of whether the entries are filtered or not filtered.

Filter Button

> Performs the filter and displays the results.

Clear Filter Button

> Removes any filters currently in effect.

Refresh Button

> Displays and updates log entries, and removes any filters. The Server Log does not refresh automatically. If the Server Log is open and new entries are written to the log, you must click **Refresh** to update the log.

File Tab

The File tab lets you specify which day's server log you wish to view. You can select the current day's log file, or a previous day's log file. The Extreme Management Center Server must be local in order to view previous logs.
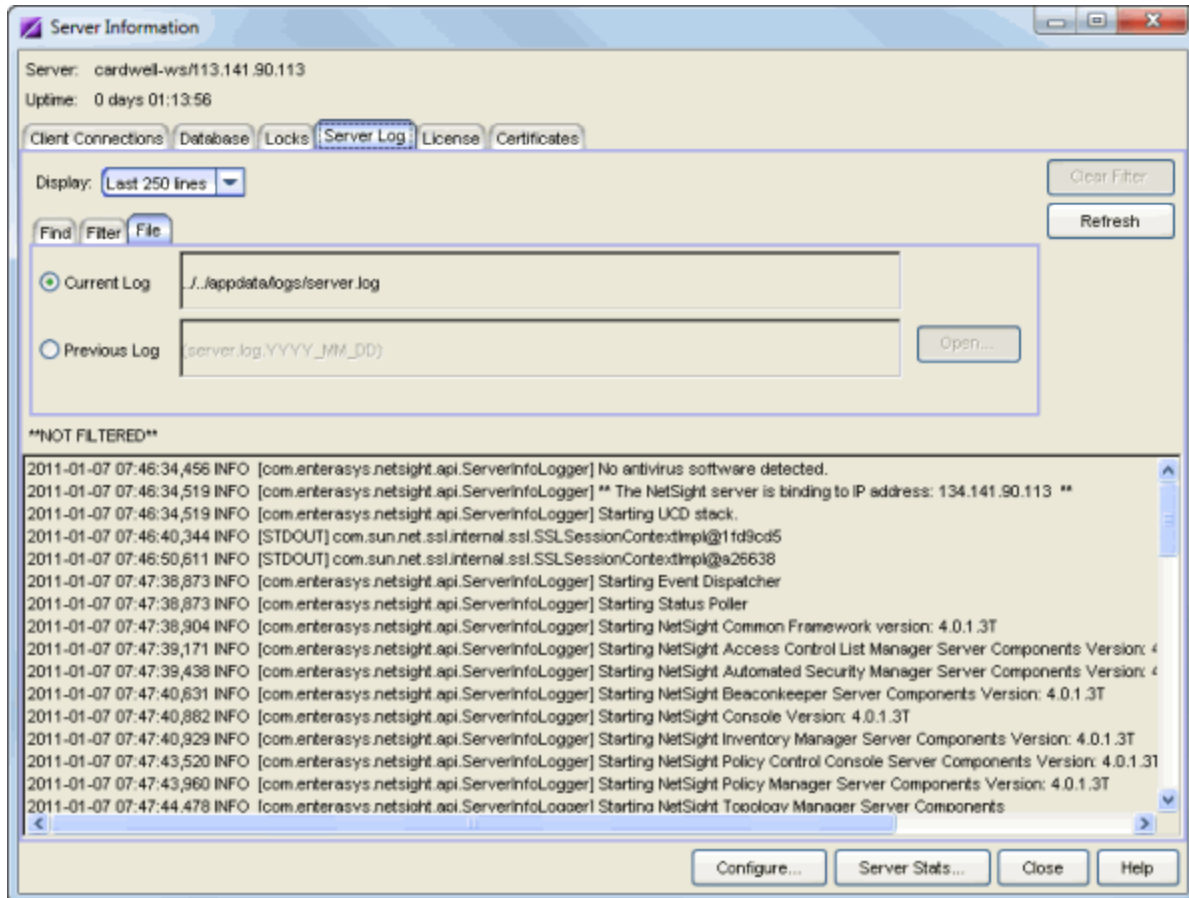
Display:

Use the drop-down list to select the number of lines you would like displayed in the log.

Current Log

Select this button to view the current day's log. The name of the log and the path to where it is located is displayed in the field to the right.

Previous Log

Select this button to view a previous day's log. Click the **Open** button to open a file selection window where you can select the log you want to view. The file names are dated, in the format `YYYY_MM_DD_events.log`. The Extreme Management Center Server must be local in order to view previous logs.

Server Log Entries

Lists the entries in the currently selected Server Log, by date and time, with the more recent entries at the bottom. If you apply a filter to the log, only the entries that match the filter are displayed on this tab.

Clear Filter Button
> Removes any filters currently in effect.

Refresh Button
> Displays and updates log entries, and removes any filters. The Server Log does not refresh automatically. If the Server Log is open and new entries are written to the log, you must click **Refresh** to update the log.

License Tab

The License tab displays a list of all licenses that are present on the Extreme Management Center server. It also lists any Extreme Access Control assessment license and Extreme Access Control VM (virtual engine) license, if applicable. See below for more information on the [Extreme Access Control VM license](#).

You can also use this tab to change a license. You would change a license in the event that you want to upgrade from an evaluation copy to a purchased copy or upgrade to a license that supports more users/devices.

Contact your Extreme Networks Representative to purchase the software and receive a Licensed Product Entitlement ID that allows you to generate a product license. Prior to changing a license, you must redeem your Entitlement ID for the new product license. Refer to the instructions included with the Entitlement that was sent to you. (For more information, view the Product Licensing information at http://www.extremenetworks.com/support/enterasys-support/how-to/ .)
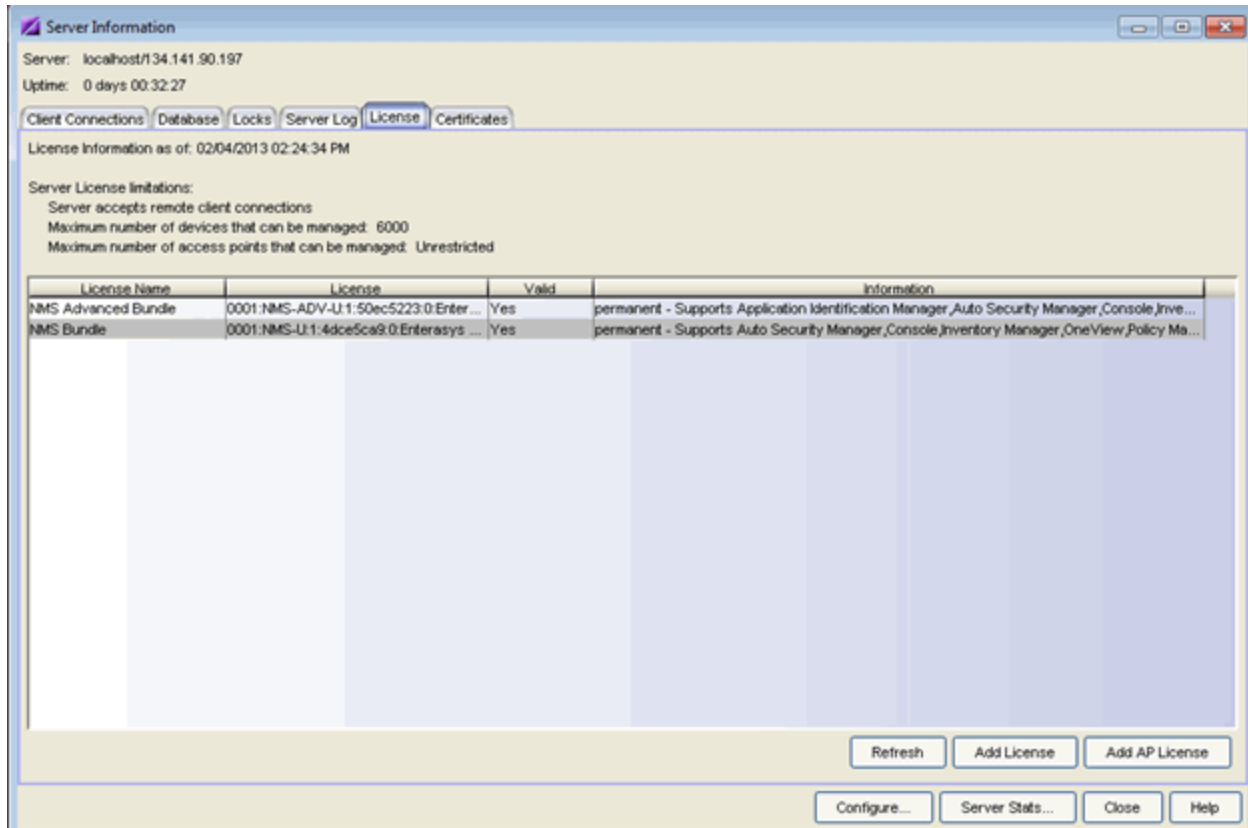
Server License Limitations

    Information on the selected server license:

- whether the server accepts connections from remote clients.

- the maximum number of devices that can be managed by the server.

- the maximum number of access points that can be managed by the server.

License Name

    Lists the Extreme Management Center (formerly NetSight) license name. It also lists any Extreme Access Control assessment license and Extreme Access Control VM (virtual engine) license, if applicable.

License

    The license number. This is the license text entered during installation.

Valid

    Whether the license is a valid license.

Information

> Displays a list of the licensed feature. If the licensed application is an evaluation copy, this column displays the date the license expires.

Refresh Button

> Refreshes the table and obtains updated license information.

Add License Button

> Opens a window where you can add a new license. Read and accept the terms of the license agreement and click **OK**. Enter the license text that you received when you generated the product license. (When you purchased your Extreme Management Center software product, you received a License Entitlement ID that allows you to generate a product license. Refer to the instructions included with the License Entitlement ID that was sent to you.) Click **Update.** The license file will be updated with the new license text.

Add AP License

> Opens a window where you can add an Access Point license. Enter the license text that you received when you generated the product license. (When you purchased your software product, you received a License Entitlement ID that allows you to generate a product license. Refer to the instructions included with the License Entitlement ID that was sent to you.) Click **Update.** The license file will be updated with the new license text.

Extreme Access Control VM License

The Extreme Access Control virtual engine requires the presence of an Extreme Access Control VM license in the Extreme Management Center Server. This license can be provided separately, as part of a bundle, or as part of an evaluation license.

The Extreme Access Control VM license includes a device limit which indicates the number of virtual Extreme Access Control engines that can be licensed. The Extreme Access Control VM license allocates license units to Extreme Access Control virtual engines according to the number of devices it supports. If a virtual engine has a license unit allocated to it, its license status is licensed; otherwise, it is unlicensed. You can see the license status for a virtual engine in the Extreme Access Control Manager engine Configuration tab or in the engine Administration web page. Additional Extreme Access Control VM licenses can be added to increase the device limit.

License units are allocated to virtual Extreme Access Control engines as follows:

- When a virtual Extreme Access Control engine is discovered, if there are any available license units, a license unit is allocated to the engine. (Extreme Management Center does not discover that an Extreme Access Control engine is virtual until it is contacted.) The number of available license units can be viewed in the License table in the Information column.

- When a licensed virtual Extreme Access Control engine is deleted, that license unit will be allocated to any unlicensed virtual Extreme Access Controlengine.

- IF the Extreme Access Control VM license is updated and license units have been added, they are allocated to unlicensed virtual engines. If license units have been removed, license units are revoked from licensed virtual engines as necessary, according to the device limit.

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.

Server Information Window

Server Certificate

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 Extreme Management Center Server Certificate](#).

Client Trust

This section displays the current client trust mode that specifies how Extreme Management Center clients handle a server certificate. Click the **Change Trust Mode** button to open the [Update Client Certificate Trust Mode window](#) where you can change the client trust mode.

Server Trust

This section displays the current server trust mode that specifies how servers handle certificates from other servers. Click the **Change Trust Mode** button to open the [Update Server Certificate Trust Mode window](#) where you can change the server trust mode.

Configure Button

Opens the Console Client Connections Options window where you can configure the maximum number of concurrent client connections supported by the Extreme Management Center Server.

Server Stats Button

Opens the Server Statistics window where you can view Extreme Management Center Server statistics such as CPU usage, and also launch Advanced statistics used for troubleshooting purposes.

Related Information

For information on related windows:

- Console Client Connections Options Window
- Server Statistics Window

Server Statistics Window

Use this window to view Extreme Management Center Server statistics. You can access the window by clicking the **Server Stats** button in the <u>Server Information window</u>.
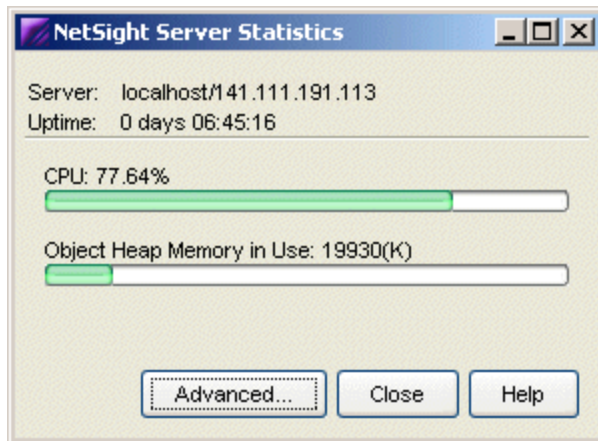
CPU

The percentage of CPU being used by the Extreme Management Center Server.

Object Heap Memory in Use

The amount of object heap memory (in kilobytes) being used by the server. Heap memory refers to the amount of free memory available to the program.

Advanced Button

Opens the <u>Advanced Statistics window</u>, which provides server statistics that can be used for troubleshooting purposes.

Related Information

For information on related windows:

- <u>Server Information Window</u>

Update Client Certificate Trust Mode Window

This window lets you update the client certificate trust mode that specifies how Extreme Management Center clients handle the server certificates they receive. You can access this window from the [Server Information Window Certificates Tab](#).
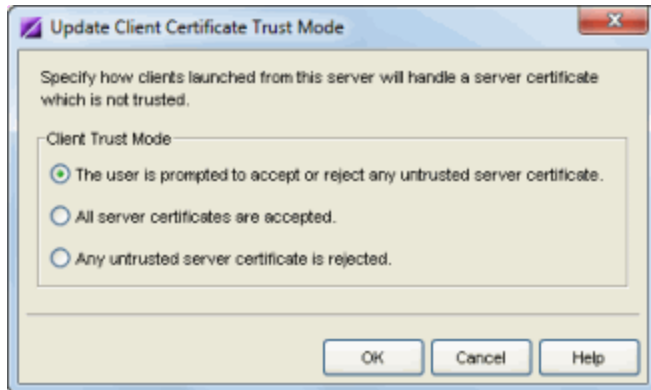
Extreme Management Center and NAC use server certificates to provide secure communication for application web pages and for internal communication between server components. When a server certificate is replaced, Extreme Management Center clients must be configured to trust the new certificate. A trust mode is used to determine how all clients handle updated certificates. You can set the client trust mode to one of the following options:

- **Prompt** (default mode) - 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 has not been replaced and the client has inadvertently connected to a server that is not trusted, then the user can reject the certificate.

- **Trust All** - All server certificates are accepted without a trust check. Use this option if there is no possibility that a client could connect to a server that is not trusted, and the user does not need to be prompted to accept or reject a new certificate.

- **Strict** - 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 will be rejected. If you are replacing a server certificate, you should not use this trust mode.

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 - Server Information Window
- Update Server Certificate Trust Mode Window

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 Server Information Window 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 Extreme Management Center 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.
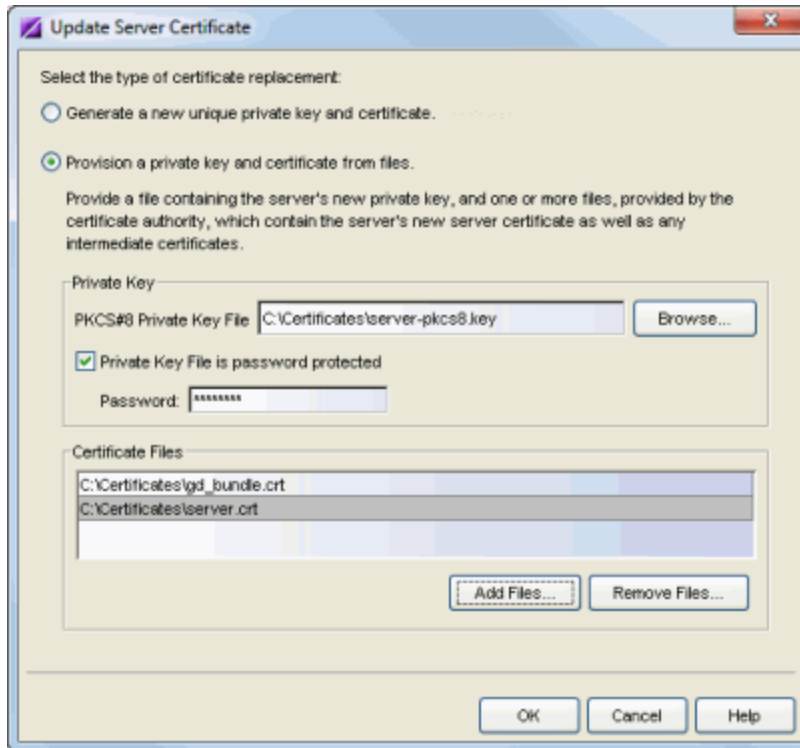
Select the type of certificate replacement

You can select from two types of certificate replacement:

- **Generate a new unique private key and certificate.** This option allows you to automatically generate a new private key and certificate using the same method that is used when Extreme Management Center is installed.

- **Provision a private key and certificate from files.** This option lets you update the server certificate to a custom certificate provided from an external certificate authority. For complete instructions on replacing and verifying the certificate using this option, see How to Update the Extreme Management Center Server Certificate.

Private Key

Provide a file containing the RSA or DSA private key that corresponds to the certificate. It must be encoded as a PKCS #8 file. Enter the path name of the file or use the **Browse** button to navigate to the file. If the file is encrypted with a password, check the password box and supply the password in the field. If you do not have the private key, refer to the instructions for generating them.

Certificate Files

Use the **Add Files** button to add one or more certificate files as provided by the certificate authority. This includes the server certificate, as well as any intermediate

or chained certificates. You can multi-select files in the file chooser window, and the files can be added in any order.

Related Information

For information on related windows:

- [Certificates Tab - Server Information Window](#)
- [Update Server Certificate Trust Mode Window](#)
- [Update Client Certificate Trust Mode Window](#)

Update Server Certificate 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. You can access this window from the [Server Information Window Certificates Tab](#).
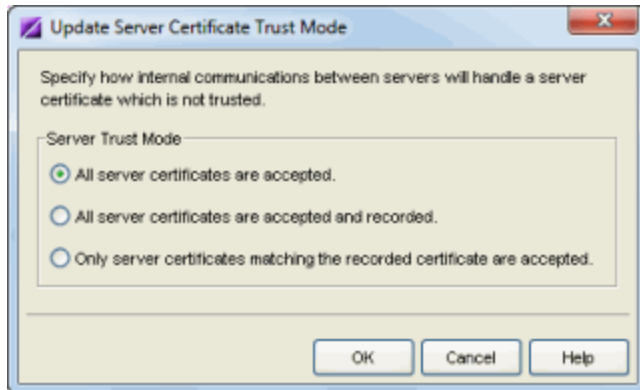
Depending on your deployment, there can potentially many servers in Extreme Management Center and NAC. For example, there is the Extreme Management Center server, the Extreme Access Control appliance servers, and Extreme Access Control assessment servers. In addition, there may be external servers such as LDAP servers that both Extreme Management Center and Extreme Access Control may communicate with. 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:

- **Trust All** (default mode) - 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.

  This mode is also useful when troubleshooting trust problems on the network. It allows the Extreme Management Center server to communicate with all Extreme Access Control appliances, and configure those appliances to accept all certificates. This restores any communication that might have been broken due to a trust issue,

and allows you to resolve the problem from NAC Manager.

- **Trust and Record** - 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.

  This mode is used initially until all servers build a complete set of certificates they need, and then the mode can be changed to Locked. 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 Locked.

- **Locked** - Any certificate from another server must match the certificate that was recorded for that server during the Trust and Record phase. 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 the "Locked" mode is the most secure, if any server certificate is replaced, the new certificate will be rejected. Therefore, if you are replacing a server certificate, you should revert back to the "Trust and Record" mode until the new certificate has been recorded.

When the trust mode is changed, the Extreme Management Center server is immediately changed to use the new mode. Extreme Access Control appliances begin using the new trust mode when they are 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 windows:

- [Certificates Tab - Server Information Window](#)
- [Update Client Certificate Trust Mode Window](#)

Table Tools

Many Extreme Management Center tables provide a set of tools that let you customize table settings and help you to find, filter, sort, print, and export information in tables. You access Table Tools, either through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools button in the upper left corner of the table (if you have the row count column displayed).

Table Tool Menu Options

Right-click menu options can include the following selections, depending on the current application and the table being viewed:

- **Hide Column** - hides a selected column. (You must right-click on a column heading to see this option.)
- **Find** - places the Find toolbar at the top of the table.
- **Filter** - places the Filter toolbar at the top of the table.
- **Sort** - places the Sort toolbar at the top of the table.
- **Insert Row** - adds a row above the selected row.
- **Delete Row(s)** - removes the selected row(s) from the table.
- **Auto Export** - places the Auto Export toolbar at the top of the table.
- **Column Filter** (Console only) - opens the **Column Filter** where you can select the information categories that appear in the table (Statistics, Configuration, Capabilities).
- **Go to View:**
    - **Device Properties** (Console only) - displays the Properties tab with Device selected to show information for selected device.
    - **Port Properties** (Console only) - displays the Properties tab with Ports selected to show information for the ports on the selected device.
- **Add Devices to Group** (Console only) - opens the Add Devices to Group window where you can select a group where you want to add the selected devices.

- **Add Port Elements to Group** (Console only) - opens the Port Group Selection window where you can select a group where you want to add the selected ports. This option is available with all FlexView tables, but should only be used with FlexViews that list ports in the table.

- **Select All** - selects all of the entries in the table.

- **Unselect All** - de-selects all of the entries in the table.

- **Port Tools**

    - **Port Monitor** (Console only) - Opens the Port Monitor window for the selected port.

    - **Interface Statistics** (Console only) - Opens the Interface Statistics window for the selected port. This menu option is available when the Instance type for this FlexView is set to **802.1D Bridge Port** or **MIB-2 Interfaces** in the FlexView properties.

- **Table Tools**

    - **Copy Selected Rows -** copies the rows selected in the table and lets you paste those rows into any application that supports a paste operation.

    - **Copy Cell** - copies the contents of the cell selected in the table and lets you paste those contents into any application that supports a paste operation.

    - **Export/Export Selection** - lets you export selected rows or the entire table to a file. The table information can be exported to an HTML file or a delimited text file. You can set the appearance of HTML exports by editing the FlexibleTable.properties file. Refer to [How to Set the Appearance of Exported Tables](#) for more information on formatting HTML tables.

    - **Page Setup** - opens the Page Setup window where you can select paper and printer options.

    - **Print/Print Selection** - lets you print selected rows or the entire table.

    - **Settings** - Opens the [Table Settings](#) window for the current table where you can choose the columns (including the row count column) that will appear in the table.

Related Information

For information on related windows:

- [Table Settings Window](#)
- [Filter Toolbar](#)
- [Find Toolbar](#)
- [Sort Toolbar](#)

For information on related tasks:

- [How to Filter, Find, and Sort](#)
- [How to Export Tables](#)
- [How to Set the Appearance of Exported Tables](#)

Auto Export Toolbar

This feature lets you automatically save the contents of tables at a specified interval. You can save the exported data in a delimited text (.csv or .txt) or HTML format.

Access the Auto Export toolbar by right-clicking anywhere in a table and selecting **Auto Export**. The toolbar appears at the top of the table.
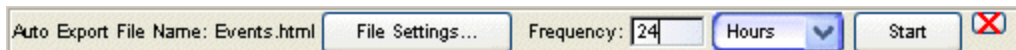
Auto Export File Name

> Select a file for your auto export. Click the **File Settings** button to open the Auto Export File Settings window where you can enter a filename, and select a destination folder and file type (HTML or a Delimited Text spreadsheet-compatible format). Select the appropriate File Management option:
>
> - Append - Appends the current data being exported to the data in the existing file.
>
> - Replace - Replaces the data in the existing file with the current data being exported.
>
> - Timestamp - Creates a new file of the same name plus the current date and time.
>
> If you have selected the delimited text file type, specify your field delimiter and text delineation options. Click **OK**. The file name will be displayed in the toolbar.

Frequency

> Set the auto export interval by entering a value and using the drop-down list to specify the unit of time.

File Settings Button

> Lets you select a file for your auto export. Opens the Auto Export File Settings window where you can enter a filename, and select a destination folder and file type (HTML or delimited text CSV spreadsheet-compatible format).

> **NOTE:** You can further customize the appearance of tables exported in HTML format using an HTML or text editor to modify the `FlexTable.properties` file. Refer to How to Set the Appearance of Exported (HTML) Tables for more information.

Start Button

Starts the auto export. The export is performed immediately and then again at the specified frequency. The Start button changes to a Stop button, allowing you to stop the auto export function, if desired. If the Frequency is set to Once, the Start button will not change to Stop.

Related Information

For information on related tasks:

- How to Export Tables
- How to Set the Appearance of Exported (HTML) Tables

How to Export Tables in Extreme Management Center

You can export information from many of the tables in Extreme Management Center applications, including the Alarms and Events Panel. The exported information can be formatted as a table in an HTML file or as a space-delimited text file. You can set the appearance of HTML exports by editing the FlexibleTable.properties file. Refer to [How to Set the Appearance of Exported Tables](#) for more information on formatting HTML tables. The procedure used to export table information is the same, regardless of the source.

To export table information:

1. Select a table that contains the information that you want to export.

2. Right click on any of the column headings or anywhere in the table body, or click the Table Tools ![icon] button in the upper left corner of the table (if you have the row count column displayed), and select **Table Tools > Export**. A file browser window opens where you can name your exported file, select the File Type (Delimited Text or HTML), and navigate to a folder/directory where you want place the file.

3. Type a name and file extension for your export file and click **OK**.

To auto export table information:

1. Select the table that contains the information that you want to export. (This feature is not available for FlexViews tables.)

2. Right click on any of the column headings or anywhere in the table body, or click the Table Tools ![icon] button in the upper left corner of the table (if you have the row count column displayed), and select **Auto Export** from the popup menu. The Auto Export File Settings window opens where you can enter a filename, and select a destination folder and file type (HTML or a Delimited Text spreadsheet-compatible format).

3. Select the appropriate File Management option:

   - Append - Appends the current data being exported to the data in the existing file.

- Replace - Replaces the data in the existing file with the current data being exported.
- Timestamp - Creates a new file of the same name plus the current date and time.

4. If you have selected the delimited text file type, specify your field delimiter and text delineation options.

5. Click **OK**. The file name will be displayed in the toolbar.

6. Set the auto export frequency by entering a value and using the drop-down list to specify the unit of time.

7. Click **Start** to start the auto export. The export is performed immediately and then again at the specified frequency. The Start button changes to a Stop button, allowing you to stop the auto export function, if desired. If the Frequency is set to Once, the Start button will not change to Stop.

Related Information

For information on related windows:

- [Auto Export Toolbar](#)

For information on related tasks:

- [How to Set the Appearance of Exported (HTML) Tables](#)

How to Filter, Find, and Sort in Extreme Management Center

You can perform filter, find, and sort operations on column entries in many of the Extreme Management Center tables.

Instructions on:

- [Filtering](#)
- [Finding](#)
- [Sorting](#)

Filtering

You can filter table entries so that only those entries matching your filter criteria are displayed in the table. You can filter the entries in a single column or in all columns, and you can apply consecutive filters.

1. Right-click on a column header, and select **Filter**. The Filter window opens at the top of the table.

2. In the **Filter** field, enter the numeric value or text string that you want to filter.

3. From the **Filter in** drop-down list, select the column you want to filter. If you select **All Columns**, the filter criteria will be applied to all entries.

4. Click **Options** to set filtering options.

    a. Click **Match as string** when filtering a text string or **Match as number** when filtering a numeric entry.

    b. Select a string option. The **String Options** change according to your *Match as* choice: **Match as string**

    - **Match whole word only** - Only text strings in the table that match the entire string entered in the **Filter on** field will be shown in the table.

    - **Match contains** - Only text strings in the table that contain the string entered in the **Filter on** field within them will be shown in the table.

- **Match does not contain** - Only text strings in the table that do not contain the string entered in the **Filter on** field within them will be shown in the table.

- **Match starts with** - Only text strings in the table that begin with the string entered in the **Filter on** field will be shown in the table.

- **Match ends with** - Only text strings in the table that end with the string entered in the **Filter on** field will be shown in the table.

Match as numeric

- **Match equal to** - Only numeric entries in the table that match exactly the value entered in the **Filter on** field will be shown in the table.

- **Match not equal to** - Only numeric entries in the table except those that are not equal to the value entered in the **Filter on** field will be shown in the table.

- **Match greater than** - Only numeric entries in the table that are greater than the value entered in the **Filter on** field will be filtered from the table.

- **Match greater than or equal to** - Only numeric entries in the table that match exactly and are greater than the value entered in the **Filter on** field will be shown in the table.

- **Match less than** - Only numeric entries in the table that are less than the value entered in the **Filter on** field will be filtered from the table.

- **Match less than or equal to** - Only numeric entries in the table that match exactly and are less than the value entered in the **Filter on** field will be shown in the table.

  c. Click **OK** to exit from the Options.

5. Click the **Match case** check box to filter based on the exact case of the text entered in the **Filter on** field.

6. Click **Filter**. All entries that do not match the filter criteria will be removed.

7. If you have already performed a filter, you can repeat steps 2 through 6 to refine your filter.

8. Click **Clear** to restore all of the table contents.

Finding

You can search for a specific value in a single column or in all columns. You can search forward or backward from your current position, and also restrict your search to match the exact case and/or whole word of the entry or expand your search to find words that begin with or contain a particular string.

1. Right-click on a column header, and select **Find**. The Find window opens at the top of the table.

2. In the **Find what** field, enter the numeric value or text string that you are seeking.

3. From the **Find in** drop-down list, select **All Columns** to search all entries or **Selected Columns** to open the **Select Columns** window where you can select a one or more specific columns. (Hold the **Shift** key when selecting multiple consecutive columns or hold the **Control** key when selecting multiple non-consecutive columns.)

4. Click **Options** to set the find options.

   a. Select a string option. The **String Options** change according to your *Match as* choice: **Match as string**
   When checked, the find options become **String Options** and the **Find what** field is treated as a text string to be matched according to the selected String Option. Numbers that appear in the string are treated as text.

      - **Match whole word only** - The first text string in the table that matches the entire string entered in the **Find what** field appears highlighted (selected) in the table.

      - **Match contains** - The first text string in the table that contains the string entered in the **Find what** field within them appears highlighted (selected) in the table.

      - **Match does not contain** - The first text string in the table that does not contain the string entered in the **Find what** field within them appears highlighted (selected) in the table.

      - **Match starts with** - The first text string in the table that begins with the string entered in the **Find what** field appears highlighted (selected) in the table.

      - **Match ends with** - The first text string in the table that ends with the string entered in the **Find what** field appears highlighted (selected) in the table.

      Match as number

When checked, the find options become **Numeric Options** and the **Find what** field is treated as a number to be matched according to the selected Numeric Options. Numbers are treated as a numeric value that can be evaluated against boolean expressions in the Numeric Options.

- **Match equal to** - The first numeric entry in the table that matches exactly the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match not equal to** - The first numeric entry in the table is not equal to the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match greater than** - The first numeric entry in the table that is greater than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match greater than or equal to** - The first numeric entry in the table that is equal to or is greater than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match less than** - The first numeric entry in the table that is less than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match less than or equal to** - The first numeric entry in the table that is equal to or is less than the value entered in the **Find what** field appears highlighted (selected) in the table.

b. Click the **Match Case** check box to search based on the exact case of the text entered in the **Find what** field.

c. Click the **Wrap search automatically** check box to continue searching beyond the top or bottom of the file. The wrap stops when the search reaches the row where it was started.

d. In the Direction box, select the direction in which you want to search: **Up** (bottom to top) or **Down** (top to bottom).

5. Click **Find**.
   The first entry that matches your search criteria is highlighted in the table. Click **Find** again to search for another entry matching the search, or select **Clear** to clear the value in the **Find** field and enter new search criteria.

Sorting

Table entries can be sorted using either of two features. The first is a single column, alpha-numeric sort. The other uses the Sort toolbar to sort on two columns to arrange entries in a table. You can sort the column entries in ascending or descending order. Text fields are sorted alphabetically, numeric fields are sorted numerically, and mixed fields are sorted alpha-numerically.

Single Column Sort

Clicking a heading title in any table automatically sorts the table in ascending or descending order for the selected column. Click once to sort in ascending order; click again to sort in descending order. An arrow appears in the heading title to indicate the order.

Multi-column Sort

The Sort toolbar lets you use two sort keys when sorting a table. Primary and Secondary keys can be defined and when there are multiple entries of the matching the primary key, the secondary sort key determines the order for those entries. To sort using the Sort toolbar:

1. Right-click on a column header, and select **Sort**. The Sort toolbar appears at the top of the table.

2. Select a Primary Sort **Column** and order (**Ascending** or **Descending**) from the drop-down list in the Primary Sort area.

3. Select a Secondary Sort **Column** and order (**Ascending** or **Descending**) from the drop-down list in the Secondary Sort area.

4. Click **Sort**. The table is arranged according to your sort criteria.

5. Click **Clear** to restore the table to its unsorted order.

Related Information

For information on related windows:

- Filter Toolbar
- Find Toolbar
- Sort Toolbar

Filter Toolbar

The Filter toolbar lets you specify which entries will be displayed in a table. You can filter the entries in a single column or in all columns, and you can apply consecutive filters.

You can access the Filter Toolbar by right-clicking on a column header and selecting **Filter**. The toolbar appears at the top of the table or if the table size is too narrow to present the entire toolbar, the toolbar will be opened as a separate window.
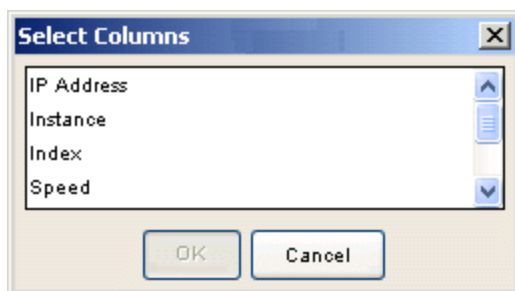

Filter on

    Enter the numeric value or text you want to filter. Clicking the **Filter** button performs the filter operation. To remove a filter, click **Clear**.

Filter in

   This drop-down list lets you choose whether to filter from **All columns** or only **Selected columns**. Select **All Columns** to filter all entries. When **Selected columns** is chosen, the Select Columns window opens where you can select one or more columns to filter.

Options

    The **Options** button opens the Options window where you can define the filter to limit the information presented in the table.
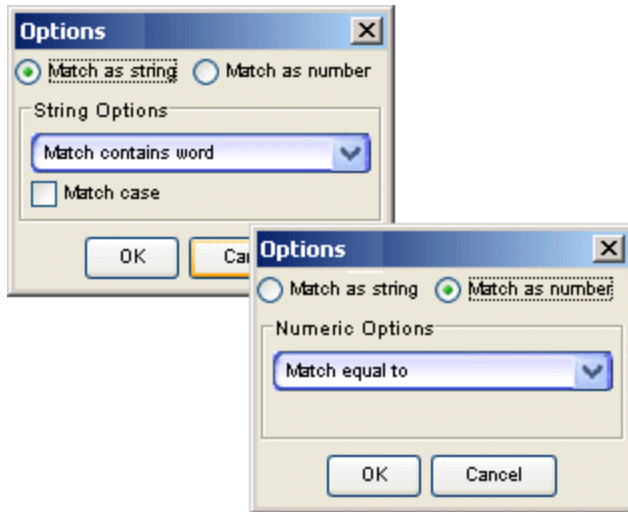
Match as string

> When checked, the filter options become **String Options** and the **Filter on** field is treated as a text string to be matched according to the selected String Option. Numbers that appear in the string are treated as text.

String Options

> These options determine how text comparisons are performed on the information in the table:
>
> - **Match whole word only** - Only text strings in the table that match the entire string entered in the **Filter on** field will be shown in the table.
>
> - **Match contains word** - Only text strings in the table that contain the string entered in the **Filter on** field within them will be shown in the table.
>
> - **Match does not contain word** - Only text strings in the table that do not contain the string entered in the **Filter on** field within them will be shown in the table.
>
> - **Match starts with word** - Only text strings in the table that begin with the string entered in the **Filter on** field will be shown in the table.
>
> - **Match ends with word** - Only text strings in the table that end with the string entered in the **Filter on** field will be shown in the table.

Match case

> When checked, strings that exactly match the case and String Options of the text entered in the **Filter on** field are filtered from the table.

Match as number

When checked, the filter options become **Numeric Options** and the **Filter on** field is treated as a number to be matched according to the selected Numeric Options. Numbers are treated as a numeric value that can be evaluated against boolean expressions in the Numeric Options

Numeric Options

These options determine how numeric comparisons are performed on the information in the table:

- **Match equal to** - Only numeric entries in the table that match exactly the value entered in the **Filter on** field will be shown in the table.

- **Match not equal to** - Only numeric entries in the table except those that are not equal to the value entered in the **Filter on** field will be shown in the table.

- **Match greater than** - Only numeric entries in the table that are greater than the value entered in the **Filter on** field will be filtered from the table.

- **Match greater than or equal to** - Only numeric entries in the table that match exactly and are greater than the value entered in the **Filter on** field will be shown in the table.

- **Match less than** - Only numeric entries in the table that are less than the value entered in the **Filter on** field will be filtered from the table.

- **Match less than or equal to** - Only numeric entries in the table that match exactly and are less than the value entered in the **Filter on** field will be shown in the table.

Filter Button

This button applies the currently defined filter options and column selections to the table.

Clear Button

Clears the information entered in the **Filter** field.

Options Button

This button opens the Options window where you can define the filter to limit the information presented in the table.

Close Button

Exits the Filter Toolbar.

Related Information

For information on related windows:

- [Find Toolbar](#)
- [Sort Toolbar](#)

For information on related tasks:

- [How to Filter, Find, and Sort](#)

Find Toolbar

The Find feature lets you locate a specific text string or value in a table. You can search in a single column or in all columns. You can also search forward or backward from your current position, and restrict your search to match the exact case and/or whole word of the entry.

You access the Find toolbar by right-clicking on a column header and selecting **Find**. The toolbar appears at the top of the table or if the table size is too narrow to present the entire toolbar, the toolbar will be opened as a separate window.
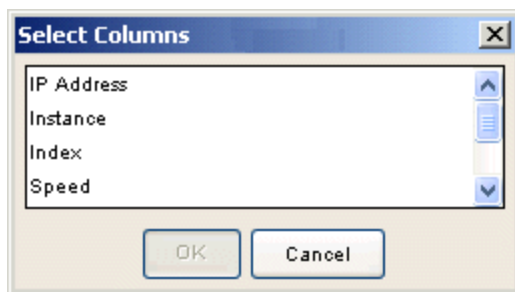

Find what
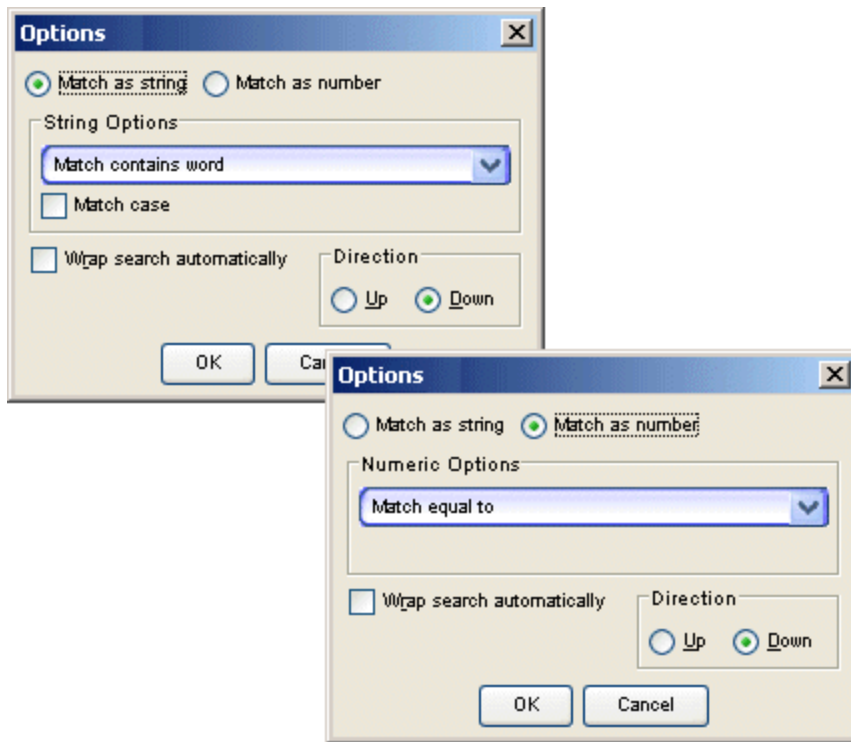
Enter the numeric value or text you want to find.

Find in

This drop-down list lets you choose, **All columns** or only **Selected columns**, where you will search for the numeric value or text in the **Find what** field. Select **All Columns** to search all entries in the table. When **Selected columns** is chosen, the Select Columns window opens where you can select one or more columns to search. The find stops with the first row that matches your **Find what** and **Find in** specification highlighted. You click Find a gain to locate the next match.

Options

This button opens the Options window where you can define the specific search criteria.

Match as string

> When checked, the find options become **String Options** and the **Find what** field is treated as a text string to be matched according to the selected String Option. Numbers that appear in the string are treated as text.

> **String Options**
>
> > These options determine how text comparisons are performed on the information in the table:
> >
> > - **Match whole word only** - The first text string in the table that matches the entire string entered in the **Find what** field appears highlighted (selected) in the table.
> >
> > - **Match contains** - The first text string in the table that contains the string entered in the **Find what** field within them appears highlighted (selected) in the table.
> >
> > - **Match does not contain** - The first text string in the table that does not contain the string entered in the **Find what** field within them appears highlighted (selected) in the table.

- **Match starts with** - The first text string in the table that begins with the string entered in the **Find what** field appears highlighted (selected) in the table.

- **Match ends with** - The first text string in the table that ends with the string entered in the **Find what** field appears highlighted (selected) in the table.

Match as number

When checked, the find options become **Numeric Options** and the **Find what** field is treated as a number to be matched according to the selected Numeric Options. Numbers are treated as a numeric value that can be evaluated against boolean expressions in the Numeric Options.

Numeric Options

These options determine how numeric comparisons are performed on the information in the table:

- **Match equal to** - The first numeric entry in the table that matches exactly the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match not equal to** - The first numeric entry in the table is not equal to the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match greater than** - The first numeric entry in the table that is greater than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match greater than or equal to** - The first numeric entry in the table that is equal to or is greater than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match less than** - The first numeric entry in the table that is less than the value entered in the **Find what** field appears highlighted (selected) in the table.

- **Match less than or equal to** - The first numeric entry in the table that is equal to or is less than the value entered in the **Find what** field appears highlighted (selected) in the table.

Match case

When checked, strings that exactly match the case and String Options of the text entered in the **Find what** field appears highlighted (selected) in the table.

Wrap search automatically

When checked, the search will continue beyond the upper or lower extremity of the table, stopping only after searching all table rows once.

Direction - Up, Down

Searches in the selected direction from the currently selected table row. Searching Up with the wrap feature disabled ends the search at the top of the table. Likewise, a Down search stops at the last table row when wrap is disabled.

Find Button

Performs the find operation. The find stops with the first row that matches the search criteria highlighted in the table. Click **Find** again to locate the next match.

Close Button

Exits the Find Toolbar.

Related Information

For information on related tasks:

- [Filter Toolbar](#)
- [Sort Toolbar](#)

For information on related tasks:

- [How to Filter, Find, and Sort](#)

Sort Toolbar

The Sort Toolbar lets you sort on two columns to arrange entries in a table.

You can access the Sort toolbar by right-clicking on a column header and selecting **Sort**. The toolbar appears at the top of the table or, if the table size is too narrow to present the entire toolbar, the toolbar will be opened as a separate window.
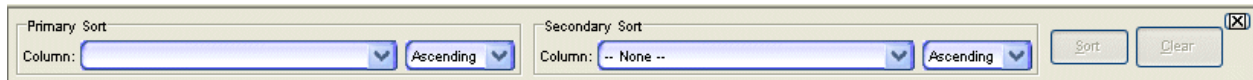
Primary Sort
> These parameters define the column and order for the primary sort key. When there are multiple entries of the same value the selected column, the secondary sort parameters will apply to determine the order for those entries.
>
> **Column**
>> This drop-down list lets you choose a column to sort.
>
> **Order**
>> This drop-down list lets you choose to sort in ascending or descending order.

Secondary Sort
> These parameters define the column and order for the secondary sort key. When there are multiple entries of the same value for the primary sort column, the secondary sort parameters will apply to determine the order for those entries.
>
> **Column**
>> This drop-down list lets you choose a column to sort.
>
> **Order**
>> This drop-down list lets you choose to sort in ascending or descending order.

Sort Button
> Performs the sort operation.

Clear Button
> Restores the table to its unsorted order.

Close Button
> Exits the Sort window.

Related Information

For information on related windows:

- [Find Toolbar](#)
- [Filter Toolbar](#)

For information on related tasks:

- [How to Filter, Find, and Sort](#)

How to Print Tables in Extreme Management Center

You can print the information from many of the tables in Extreme Management Center applications. The procedure used to print the table information is the same, regardless of the source. You can print selected rows or the entire table.

Select rows:

1. Select the rows in the table that you want to print or go on to Step 2 to print the entire table. You can select multiple rows by either holding the Control key while clicking non-consecutive rows or holding the Shift key while clicking the first and last row in a desired range of rows.

Print table information:

2. Right click on any of the column headings or anywhere in the table body, or click the Table Tools button in the upper left corner of the table (if you have the row count column displayed), and select **Table Tools > Print**. The Page Setup dialog window opens.

3. Select your page setup options according to the size and layout of your table information and click **OK**.

4. In the Print dialog window, set your print options and click **OK**.

Related Information

For information on related windows:

- Table Tools

For information on related tasks:

- How to Filter, Find, Sort
- How to Export Tables
- How to Set Table Properties

How to Set the Appearance of Exported (HTML) Tables in Extreme Management Center

The tables in many of the views in Extreme Management Center applications can be exported as an HTML file using the Export and Auto Export features. The `FlexibleTable.properties` file is where you can customize the appearance of tables that are exported as html. In the file, you can define specific elements in the html table tags used to format the exported data.

To customize your exported table formats:

1. The FlexibleTable.properties file is included in the commonui.jar located in *<install directory>* `/jboss/server/default/deploy/NetSight/Clients.war/plugins/ common.` It is not extracted by default during an installation. You can extract that file from the jar (or create your own) and place it in the platform dependent <user home dir>/NetSight/Console directory. From that directory you can open the file in your favorite text editor and make any desired changes. Note that any changes to the file must be made before Extreme Management Center clients are launched, or they will not take effect.

2. Edit the table format parameters. You can define four table elements:

   - **TableFormat** - defines the overall appearance (alignment, background, borders, etc.) for the table.
   - **TableHeaderFormat** - defines the appearance of the header row.
   - **TableOddRowFormat** - defines the appearance of the odd table rows.
   - **TableEvenRowFormat** - defines the appearance of the even table rows.

   You can set these properties to any attribute that is legal for version 3.2 and 4.0 HTML table tags.

   For example, the following entries define attributes for the overall table style and the fonts and backgrounds for the header and the odd and even table rows to produce the table shown below.

   TableFormat= align="Left" border="0" style="border-style:Groove"
   TableHeaderFormat= style="background-color:Silver;font-size:8pt;font-

weight:bold;font-style:Italic;" align="Center"
TableOddRowFormat= style="background-color:White;font-size:8pt;"
TableEvenRowFormat= style="background-color:Gainsboro;font-size:8pt;"

Last Update: 07/15/2004 09:07:58 AM EDT

IP Address	Interface	Name	Type	Description
10.20.150.80	1	Ethernet Frontpanel	ethernetCsmacd	Ethernet Frontpanel
10.20.150.81	1	Ethernet Frontpanel	ethernetCsmacd	Ethernet Frontpanel
10.20.150.75	1	-	ethernetCsmacd	Gigabit Ethernet Frontpanel port 1
10.20.150.100	1	fe.1.1	ethernetCsmacd	Fast Ethernet Frontpanel
10.20.150.76	1	fe.0.1	ethernetCsmacd	Fast Ethernet Frontpanel port 1
10.20.33.1	1	et.4.1	ethernetCsmacd	Physical port: et.4.1
10.20.150.77	1	Fast Ethernet Frontpanel	ethernetCsmacd	Fast Ethernet Frontpanel
10.20.150.78	1	Ethernet Frontpanel	ethernetCsmacd	Ethernet Frontpanel
10.20.150.1	1	et.3.1	ethernetCsmacd	Physical port: et.3.1
10.20.150.130	1	XMIB2_NAME_STR	ethernetCsmacd	RMON Port 1 on Unit 1
10.20.150.79	1	Ethernet Frontpanel	ethernetCsmacd	Ethernet Frontpanel
10.20.33.3	1	Fast Ethernet Frontpanel	ethernetCsmacd	Fast Ethernet Frontpanel
10.20.33.4	1	Ethernet Frontpanel	ethernetCsmacd	Ethernet Frontpanel
10.20.150.2	1	et.1.1	ethernetCsmacd	Physical port: et.1.1
10.20.33.6	1	-	ethernetCsmacd	Ethernet Frontpanel

3. Save your changes. Exported tables will be formatted with your changes.

Related Information

For information on related windows:

- Auto Export Toolbar

For information on related tasks:

- How to Filter, Find, Sort
- How to Export Tables

How to Set Table Settings in Extreme Management Center

The Table Settings Window allows you to customize the tables that appear in Extreme Management Center applications.

Open the **Table Settings** Window:

1. Right click on any of the column headings or anywhere in the table body and select **Table Tools > Settings**.

2. Select **Yes** or **No** to show or hide the row count column. The row count column and Table Tools button appear as the left-most column in the table.

3. In the **Hide** column, use the checkboxes to select which columns will be displayed and which will be hidden.

4. Click **Apply** to confirm your selections.

5. Click **Close** to dismiss Table Settings the window.

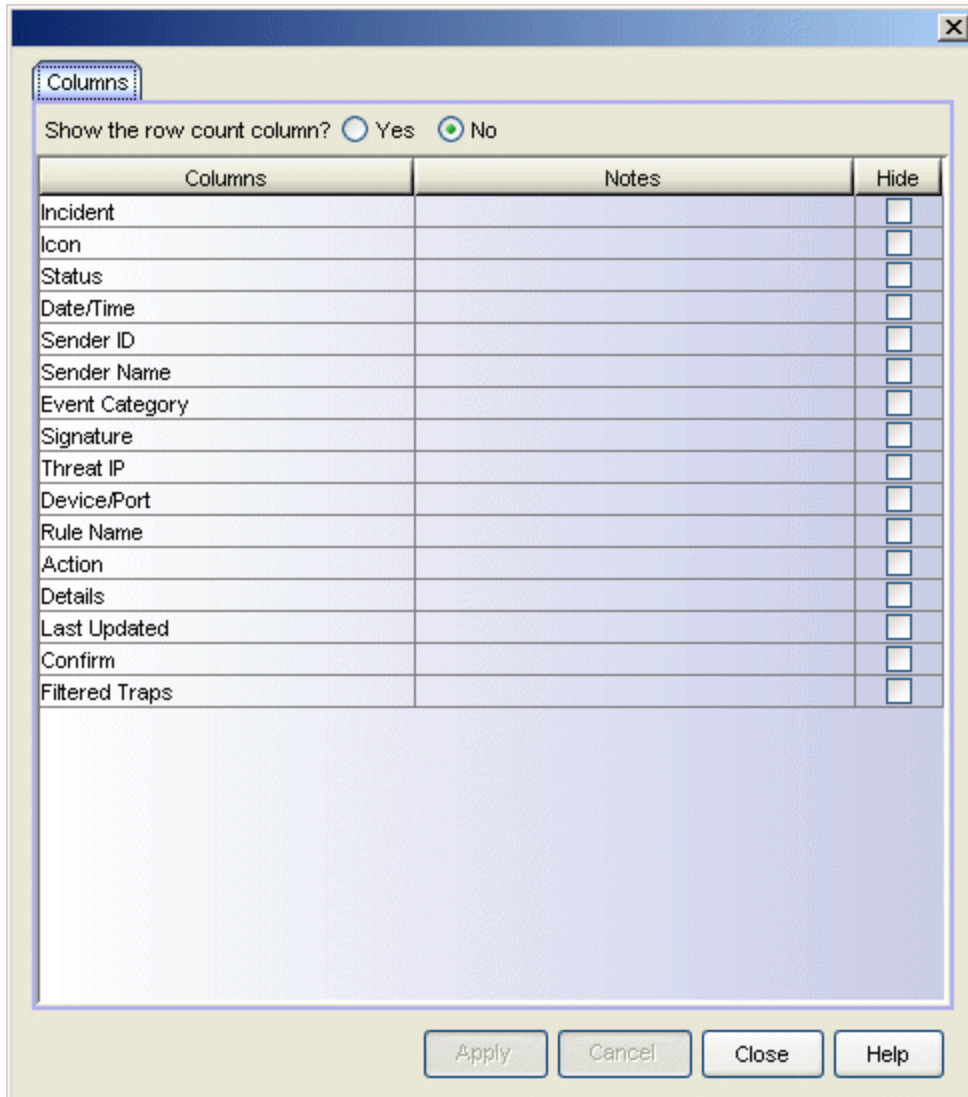**Related Information**

For information on related windows:

- Table Settings Window

For information on related tasks:

- How to Filter, Find, Sort
- How to Export Tables
- How to Print Tables

Table Settings Window

This window lets you choose the columns that will appear in the current table using the checkboxes in the Hide column.

Show the row count column?

>   This feature allows you to show or hide the row count column and Table Tools button that appear as the left-most column in the table.

Columns

>   Displays the available columns for the current table.

Notes (Console FlexViews only)

This column displays notes that were entered for columns created in Console's FlexView Properties window.

Hide

Use the checkboxes to select which columns will be displayed and which will be hidden in the current table.

Related Information

For information on related windows:

- Filter Toolbar
- Find Toolbar
- Sort Toolbar

For information on related tasks:

- How to Filter, Find, and Sort
- How to Export Tables
- How to Set the Appearance of Exported Tables

Troubleshooting

This troubleshooting guide provides a list of items to check when certain Extreme Management Center functionality is failing to perform correctly.

Locate a problem in the left column and then review the troubleshooting steps in the right column.

Problem	Troubleshooting Steps
Linux: Remote Clients Unable to Connect	On Linux, if a client can connect locally to the Extreme Management Center Server, but remote clients are unable to connect, here are some things to check:

1. Log on to the Extreme Management Center Server as root and check the following sockets using the command:

   `netstat -pel | grep <socket>`

   a. Check the socket 4588:

      `netstat -pel | grep 4588`

      This socket should be in LISTEN mode - *localhost:4588 listen*.

   b. Check the socket 4589:

      `netstat -pel | grep 4589`

      This socket should be in LISTEN mode - *localhost:4589 listen*. If either socket is not in LISTEN mode, then it is likely that the database has failed to start, or that the server did not load properly. If this happens, consult the server log, these problems generate traces.

   c. Check the socket 4532:

      `netstat -pel | grep 4532`

      This socket should be in LISTEN mode - **:4532*. If it is anything but asterisk (*) (eg., *localhost:4532*, or *127.0.0.1:4532*), the server is listening locally.

2. If DNS is enabled on the system:

   a. Open the file:
      `<install directory>/appdata/NSJBoss.properties` and add the entry:
      `sun.net.spi.nameservice.provider.1=dns,sun`

   b. Restart the Extreme Management Center Server.

   NOTE: If this change is made when DNS cannot correctly resolve the hostname, the Extreme Management Center Server does not start properly.

3. If DNS is not enabled on the system:

   a. Open the `/var/Extreme_Networks/.netsight` file. Look for a device hostname configuration.

| | b. Edit the line `JBOSS_HOSTNAME=` to add your hostname. For example: `JBOSS_HOSTNAME="1.2.3.4"` |

c. Restart the Extreme Management Center Server.

If the problem persists, contact Extreme Networks Support at http://www.extremenetworks.com/support/.

| Windows: Client unable to connect | On Windows, if a server system has multiple NICs (Network Interface Cards) installed, the binding order for local host must be properly configured or the local client may be unable to connect to the server and remote clients may be unable access the Extreme Management Center Launch Page. |

Set the binding order of multiple network interface cards and configure the Extreme Management Center Server to bind to the correct IP address. These steps may vary depending on your operating system.

1. Open the Network Connections window:

   a. Click Start > Run

   b. Enter `ncpa.cpl` and click OK.

   The Network Connections window opens. You can view the available connections in the LAN and High-Speed Internet section of the window.

2. From the Network Connections window menu bar, select Advanced > Advanced Settings. The Advanced Settings window opens.

3. The Adapters and Bindings tab lists the connections in the order in which the connections are accessed by network services. The NIC that the Extreme Management Center server should connect to must be first in the list. You can use the arrow buttons to change the binding order.

4. Open the `.netsight` file. Edit the line `JBOSS_HOSTNAME=<server IP>` to add your server IP address. (On Windows Server 2008 and Windows 7, the file is located at C:\ProgramData\Extreme Networks. On Windows Server 2003 and Windows XP, the file is located at C:\Documents and Settings\All Users\Application Data\Extreme Networks.)

5. Restart the Extreme Management Center Server.

Problem	Troubleshooting Steps
Extreme Management Center user is denied access to specific Extreme Management Center functions or operations.	Use the following steps to troubleshoot issues where Extreme Management Center users are unable to access Extreme Management Center functionality.

1. Verify that the user's login credentials match those in the database and that the user logged in with the correct domain and username combination. Generally, authenticating to a Linux platform server requires the username and authenticating to a Windows platform server requires a domain name\username. The login is case-sensitive, so the exact case should be used.

2. Verify that the user is a member of an authorization group that has been granted the capability to access the operation in question. For more information on authorization capabilities, see the Extreme Management Center online Help topic How to Configure User Access to Extreme Management Center Applications.

3. Obtain detailed Authentication debug information by setting the Authentication Diagnostic Level to Verbose in the Extreme Management Center Launch Page > Administration tab > Server Diagnostics tab. Access the debug information in <install directory>\appdata\logs\server.log on the Extreme Management Center Server.