



# **Extreme Networks Extreme Management Center<sup>®</sup>**

***Console User Guide***



Copyright © 2016 Extreme Networks, Inc. All Rights Reserved.

## 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/](http://www.extremenetworks.com/company/legal/trademarks/)

## Support

For product support, including documentation, visit: [www.extremenetworks.com/support/](http://www.extremenetworks.com/support/)

## Contact

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

Toll-free: +1 888-257-3000



## Extreme Networks® Software License Agreement

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

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

and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.
4. LICENSE TYPES.
  - *Single User, Single Computer.* Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
  - *Client.* Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to

Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED

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

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

7. TITLE AND PROPRIETARY RIGHTS

- a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers.

This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

- b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

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

of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.
10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
  - a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
  - b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in



accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

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

to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
15. GENERAL.
  - a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
  - b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
  - c. You represent that You have full right and/or authorization to enter into this Agreement.
  - d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.
  - e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
  - f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
  - g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
  - h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other

communication to be sent to Extreme must be mailed by certified mail to the following address:

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

# Table of Contents

---

- Legal Notices ..... i
- Trademarks ..... i
- Support ..... i
- Contact ..... i
- Extreme Networks® Software License Agreement ..... ii
- Table of Contents ..... x
- Extreme Management Center Console Help ..... 1
  - Management Center Console Features ..... 1
  - Document Version ..... 3
- Console Configuration Considerations ..... 5
- Getting Started with NetSight Console ..... 6
  - NetSight Console Overview ..... 8
    - Take a Look Around ..... 8
    - Main Window ..... 8
      - Menus ..... 9
      - Toolbar ..... 9
      - Left (tree) Panel ..... 10
      - Right (tabbed) Panel ..... 10
      - Event View Panel ..... 11
      - Status Bar ..... 11
- Beginning To Use Console's Features ..... 12
  - Setting Console Options ..... 12
  - Setting Access Privileges ..... 13
    - Defining User Access to Extreme Management Center ..... 14
    - Establishing Device Access (Credentials and Profiles) ..... 14

---

Populating the NetSight Database .....	15
Discovering Devices .....	16
Adding Devices Manually .....	19
Using Compass .....	20
Monitoring Alarms and Events .....	21
Working with FlexViews .....	23
Where to Go from Here .....	26
Accessing NetSight Console Help .....	26
<b>NetSight Console Concepts .....</b>	<b>28</b>
VLAN Concepts .....	29
Egress Rules (Transmitting Frames) .....	29
Dynamic Egress .....	30
GVRP .....	33
GARP Timers .....	33
Enforcing .....	33
Frame Types .....	34
IGMP .....	35
IGMP Intervals .....	35
Ingress Filtering .....	36
Priority Classification .....	36
Weighted Priority .....	37
Verifying .....	37
VLAN Identification .....	38
VLAN ID (VID) .....	38
PVID (Port VLAN ID) .....	38
VLAN Model .....	39

---

VLAN Learning .....	39
Traps and Informs .....	40
SNMPv3 Traps .....	40
SNMPv3 Informs .....	41
<b>FlexViews .....</b>	<b>43</b>
How to Use FlexViews .....	44
Opening a FlexView .....	44
Printing a FlexView Table .....	45
Exporting FlexView Data .....	46
Working with FlexView Graphs .....	47
Viewing Pie Graphs and Bar Graphs .....	47
Viewing Line Graphs .....	48
Exporting Graphs .....	51
Printing Graphs .....	51
Editing Writable Values .....	52
Using the Guided Editor .....	52
Using the Table Editor .....	52
Adding Instances in MIB Tables .....	53
How to Create and Modify FlexViews .....	56
Creating a FlexView .....	56
Modifying a FlexView .....	63
Adding and Removing FlexView Tabs .....	64
Adding Tabs .....	64
Removing Tabs .....	65
FlexView Tabs .....	66
FlexView Toolbar .....	67

---

FlexView Table .....	70
Right-Click Menu .....	70
Console Main Toolbar Buttons .....	70
FlexView Bar Graphs .....	72
Bar Graph Settings .....	73
FlexView Line Graphs .....	76
Line Graph Settings .....	77
General Controls Tab .....	77
Line Graph Controls Tab .....	79
FlexView Pie Graphs .....	82
Pie Graph Settings .....	83
How to Export a FlexView Catalog .....	86
How to Export FlexViews to a Web Monitor .....	87
FlexView Properties Window .....	88
General Tab .....	88
Columns Tab .....	91
Columns Tab - SNMP .....	92
MIB Object Selector .....	92
Columns Tab - Expression .....	96
Column Routine and Function Panel .....	97
Expression Wizard .....	98
Expression/Notes Panel .....	109
Status .....	109
Column Definitions Table .....	110
Advanced FlexView Features .....	112
FlexView Request Groups .....	112

---

FlexView Indirect Instancing .....	114
FlexView Extract Instance .....	116
FlexView Expression Editor .....	117
The Language of FlexView Expressions .....	118
Expressions .....	118
Values .....	119
Casting .....	120
Explicit Conversions .....	120
Implicit Conversion .....	121
Binary Arithmetic Conversions .....	121
Comparison Conversions .....	122
Constants .....	122
Operators .....	123
Post-unary Arithmetic Operators .....	123
Pre-unary Arithmetic Operators .....	124
Binary Arithmetic Operators .....	124
Bit-wise Operator .....	125
Comparison Operators .....	125
Logical Operators .....	126
Conditional Operators .....	126
Assignment Operators .....	126
Parenthetical Expressions .....	127
Order of Operations .....	127
Column References .....	128
Variable References .....	129
Function References .....	130



---

<b>How To Use NetSight Console</b> .....	<b>137</b>
How to Add, Remove, and Delete Devices .....	138
Adding Devices to a Group .....	138
Adding Devices Manually .....	138
Adding Devices to a Group from a FlexView Table .....	139
Copying and Pasting Devices .....	140
Dragging and Dropping Devices .....	141
Removing Devices from a Group .....	141
Deleting Devices from the NetSight Database .....	142
How to Add and Remove Port Elements .....	143
Adding Ports to a Group .....	143
Adding Selected Ports From a FlexView Table .....	143
Copying and Pasting Devices .....	144
Dragging and Dropping Ports .....	144
Removing Ports from a Group .....	145
Deleting Port Elements .....	145
How to Add MIBs to Extreme Management Center .....	146
How to Add, Remove, and Rename Groups .....	149
Adding a Group .....	149
Renaming a Group .....	149
Removing a Group .....	149
How to Add Third-Party Application Support .....	151
How to Assign ACLs to Device Interfaces and Agent Services .....	155
Assigning ACLs to Interfaces .....	155
Assigning ACLs to Agent Services .....	156
How to Clear Threshold Alarms .....	158

---

Clearing OneView Threshold Alarms .....	158
Clearing Application Analytics Threshold Alarms .....	159
How to Configure Alarms in Alarms Manager .....	160
Defining an Alarm .....	161
Disabling Alarms .....	165
Viewing Alarms .....	165
Console .....	165
Console Device Tree .....	166
Console Device Current Alarms .....	167
Console Alarms Event View .....	167
Extreme Management Center .....	168
Extreme Management Center Alarms and Events Tab .....	168
Extreme Management Center Network Tab .....	169
Clearing Alarms .....	170
How to Configure Custom Alarm Criteria .....	172
How to Configure the SNMP Trap Service .....	175
Configuring Trap Receivers .....	175
Configuring the snmptrapd.conf File .....	177
Restarting the SNMP Trap Service .....	178
How to Create ACL Rules .....	180
Creating a Rule .....	180
Modifying a Rule .....	181
Commenting and Uncommenting a Rule .....	181
Deleting a Rule .....	181
How to Discover Devices .....	183
Configuring Ping for Linux and Mac OS X Clients .....	184

---

IP Range Discover .....	184
CDP Seed IP Discover .....	188
How to Download Firmware .....	191
How to Enforce ACLs .....	193
How ACL Names are Determined on a Device .....	193
How to Export and Import a Device List .....	195
Import-Export File Format .....	195
SNMPv1/v2 .....	195
SNMPv3 .....	197
How Credentials and Profiles are Handled when Importing a Device List	198
From NetSight Console .....	198
From Ridgeline .....	199
Exporting a Device List .....	199
From NetSight Console .....	199
From Ridgeline .....	199
Importing a Device List from a File .....	200
How to Import ACL Data .....	201
Importing ACL Data From Devices .....	201
Importing ACL Data From an RSD File .....	202
How to Manage ACLs .....	203
Creating an ACL .....	203
Copying an ACL .....	204
Moving an ACL .....	205
Translating ACLs .....	205
Renaming an ACL .....	206
Editing an ACL .....	207

---

Deleting Rules .....	207
Rearranging Rules .....	208
Deleting an ACL .....	208
Creating an ACL Folder .....	208
How to Save and Restore Configuration Files .....	210
Saving Configuration Files .....	210
Restoring Configuration Files .....	212
Saving Bootlog Files .....	213
How to Set Console Options .....	216
Device Manager .....	216
Discover .....	217
FlexView .....	217
Welcome View .....	218
Property View .....	219
Compass .....	219
VLAN View .....	220
Basic Policy View .....	221
Wireless Manager .....	222
Policy Control Console .....	223
RoamAbout Wireless Manager .....	223
TopN Collector .....	224
NetFlow Collection .....	224
OneView .....	226
OneView Dialog Boxes .....	227
OneView Collector .....	227
OneView Engine .....	229

---

ACL Manager View .....	230
How to Translate ACLs and Rules .....	233
Paste and Translate ACL(s) .....	233
Translating Rules .....	234
How to Use Compass .....	236
Accessing Compass .....	237
Searching .....	237
Auto Searching .....	237
Searching All .....	237
Searching IP Addresses .....	238
Searching IP Subnets .....	238
Searching MAC Addresses .....	239
Searching Multicast Addresses .....	240
Searching User Names .....	241
Pinging .....	241
How to Use MIB Tools .....	243
Contacting a Device .....	243
Searching for MIB Objects .....	244
Querying MIB Objects .....	245
Clearing Query Results .....	245
Setting MIB Objects .....	246
Adding Rows in MIB Tables .....	247
Adding MIBs to the MIB Tools Database .....	247
MIB Tools Overview .....	248
How a MIB is Organized .....	248
How MIB Tools Works .....	250

---

How to Verify ACLs .....	252
Verifying ACLs .....	252
Resolving Differences .....	252
Working in the Left Panel .....	255
Using Cut, Copy, and Paste .....	255
Using Drag and Drop .....	255
How to Work with VLAN Models .....	257
Creating a VLAN Model .....	258
Creating a VLAN .....	258
Removing a VLAN from a VLAN Model .....	259
Creating a Port Template .....	260
Removing a Port Template from a VLAN Model .....	260
Working with VLAN Model Settings and Device VLAN Settings .....	261
Verifying VLANs .....	261
Updating VLAN Definitions from Device Settings .....	262
Enforcing VLANs .....	262
Verifying Port Templates .....	263
Updating a Port Template from Port Settings .....	264
Setting Egress States .....	264
Enforcing Port Settings .....	265
Renaming Models, VLANs, and Port Templates .....	265
Editing Port VLAN Settings .....	266
Deleting a VLAN Model .....	267
Configuring VLANs on an X-Pedition Router .....	268
Creating VLANs on X-Pedition Routers .....	268
Modifying VLANs on X-Pedition Routers .....	273

---

Removing a VLAN from a VLAN Model .....	273
Editing Port VLAN Settings .....	274
Deleting a VLAN Model .....	275
<b>Extreme Management Center Console Windows .....</b>	<b>277</b>
ACL Editor .....	278
Left-Panel Tree .....	278
ACL Details Tab .....	280
Editor Tab .....	281
Description Tab .....	285
Targets Tab .....	287
CLI Preview Tab .....	288
ACL Manager Database Properties Window .....	290
ACL Packet Evaluation Tool .....	291
Pre-Defined Well-Known IDs Window ACL Manager .....	294
Port Tab .....	294
IP Protocol Tab .....	296
ACL Manager Tab .....	298
Device Summary .....	299
Interface Assignment .....	300
Agent Assignment .....	303
Detail Log .....	306
ACL Rules Summary .....	308
ACL Rule Translation View .....	309
ACL Translation View .....	311
ACL Verification Results Window .....	313
Add Device Window .....	316

---

Add Device(s) to a Group Window .....	318
Add to ACL / Edit ACL Window .....	319
AH, ESP, or GRE Rules .....	319
ICMP or IP Rules .....	322
IPINIP Rules .....	325
IP-Protocol Rules .....	328
Standard Rules .....	331
TCP or UDP Rules .....	333
Alarm Group Selection Window .....	338
Alarm History Window (Legacy) .....	339
Alarm Limits .....	340
Alarm History Options .....	341
Alarms Manager Window .....	342
Alarm Details .....	343
Criteria Subtab .....	344
Actions Subtab .....	345
Other Options Subtab .....	347
Basic Policy Tab (Default Port Role View) .....	349
Table Editor .....	351
Basic Policy Tab (End User Sessions View) .....	353
Column Filter Toolbar .....	359
Compass Tab .....	361
Search Log Tab .....	362
Results Tab .....	362
Right-click Menu .....	363
User Location Information .....	364



---

Status Bar .....	364
Compass Tab All Search .....	365
Search Parameters .....	367
Search Log Tab .....	367
Results Tab .....	367
Compass Tab Auto Search .....	370
Search Parameters .....	371
Search Log Tab .....	372
Results Tab .....	372
Compass Tab IP Address Search .....	375
Search Parameters .....	376
Search Log Tab .....	377
Results Tab .....	377
Compass Tab IP Subnet Search .....	379
Search Parameters .....	381
Search Log Tab .....	381
Results Tab .....	381
Compass Tab MAC Address Search .....	384
Search Parameters .....	385
Search Log Tab .....	386
Results Tab .....	386
Compass Tab Multicast Address Search .....	389
Search Parameters .....	390
Search Log Tab .....	391
Results Tab .....	391
Compass Tab User Name Search .....	393

---

Search Parameters .....	394
Search Log Tab .....	395
Results Tab .....	395
Configuration Upload/Download Window .....	398
Current Device Settings .....	399
Operation .....	400
Download Settings .....	401
Status .....	402
Extreme Management Center Console Options (Legacy) .....	405
Device Manager .....	405
Discover .....	406
FlexView .....	407
For All Users .....	408
For Current User .....	408
Welcome View .....	409
Property View .....	410
Compass .....	411
VLAN View .....	413
Basic Policy View .....	415
Wireless Manager .....	416
Policy Control Console .....	417
RoamAbout Wireless Manager .....	418
TopN Collector .....	419
NetFlow Collection .....	421
OneView .....	423
OneView Dialog Boxes .....	425

---

OneView Collector .....	425
Wireless Collection .....	426
Device Collection .....	427
Interface Collection .....	427
NAC Collection .....	427
OneView Engine .....	428
ACL Manager .....	429
Discover Window .....	434
Configuring Ping for Linux and Mac OS X Clients .....	434
IP Range Discover .....	435
IP Range Tab .....	436
Right-click Menu .....	439
CDP Seed IP Discover .....	439
CDP Seed IP Tab .....	440
Discover Results Table .....	442
Status Bar .....	445
Right-click Menu .....	445
Edit Action Overrides Window .....	447
Keyword Definitions .....	448
Edit Custom Alarm Criteria Window .....	451
Edit Flow Criteria Window .....	454
Edit Threshold Window .....	457
OneView Threshold Alarm .....	457
Application Analytics Threshold Alarm .....	459
E-Mail Configuration Window .....	464
Firmware Image Download Window .....	466

---

Current Device Settings .....	467
Operation .....	468
Download Settings .....	468
Status .....	469
Flow Sensor Configuration Window .....	471
Guided Editor Window .....	474
Import This Definition Window .....	476
Main Window .....	478
Main Window Left Panel .....	481
My Network .....	481
System-Created Groups .....	481
User-created Groups .....	482
Left Panel Icons .....	482
Right-click Menus .....	482
Main Window Right Panel .....	486
Match Host Window .....	488
Match Phrase List Window .....	490
Menus .....	492
Main Window Menu Bar .....	492
File Menu .....	492
Edit Menu .....	493
Tools Menu .....	494
Applications Menu .....	495
Help Menu .....	496
MIB Tools Window .....	498
MIB Tools Device .....	499

---

MIB Tools Select Protocol .....	501
MIB Tools Tree Tab .....	502
MIB Tools List Tab .....	504
MIB Tools Details Tab .....	505
MIB Tools Current Object .....	507
MIB Tools Results Table .....	508
MIB Tools Edit Credentials Window .....	512
MIB Tools Options Window .....	514
Device Tab .....	514
Object Tab .....	514
SNMP Tab .....	515
NetFlow Advanced Settings Window .....	516
OneView Collector Advanced Settings Window .....	518
OneView Engine Advanced Settings Window .....	521
Ping Window .....	523
Port Group Selection Window .....	525
Port Monitor Window .....	526
Properties Tab .....	530
Properties Tab (Device) .....	530
Right-Click Menu .....	532
Properties Tab (Access) .....	533
Right-Click Menu .....	536
Properties Tab (Date/Time) .....	537
Right-Click Menu .....	539
Properties Tab (Ports View) .....	539
Right-Click Menu .....	546

---

Status Bar .....	547
Syslog Receiver Configuration Window .....	548
Syslog Applications Window .....	553
Main Window - Toolbar .....	555
TopN Collector Advanced Settings Window .....	557
Trap Receiver Configuration Window .....	559
Configuration Tab .....	559
snmptrapd Tab .....	564
Trap Selection Window .....	570
VLAN Definitions .....	572
VLANs in VLAN Model .....	573
VLAN Definition .....	575
IGMP Parameters .....	576
VLAN Details Window .....	578
VLAN Model and Device Table .....	579
VLAN Egress Details Window .....	581
VLAN Egress Details Table .....	581
VLAN Elements Editor .....	584
VLAN Model .....	587
VLAN Port Template Definitions View .....	589
VLAN Port Templates .....	590
Port Template Properties .....	592
VID Table .....	594
VLAN Tab (Advanced Port) .....	597
Upper Panel .....	598
Ports Table .....	599

---

Lower Panel .....	601
Port Template Table .....	602
Actual Port Settings on Device .....	602
VLAN Tab (Basic Port) .....	604
Ports Table .....	605
Custom/Port Template .....	607
VLAN Tab (Device) .....	608
Upper Panel .....	609
Device VLANs Table .....	610
Lower Panel .....	612
VLAN Definitions for Model .....	612
VLANs Definitions for Device .....	614
<b>Reference Information .....</b>	<b>617</b>
Compass SNMP MIBs Descriptions .....	618
How to Add Trap Definitions .....	622
NetSight Data Synchronization .....	623
Extreme Management Center Log Files .....	624
Extreme Management Center Application Logs .....	624
Syslog Log .....	625
Traps Log .....	625
Server Log .....	626
<b>Device Manager Help .....</b>	<b>627</b>
Device View .....	628
Menu Bar .....	630
Device Menu .....	630
View Menu .....	633

---

Utilities Menu .....	635
Help Menu .....	635
Port Display .....	637
Module/Device Menu .....	638
Port Menu .....	638
Device Information .....	639
How To Use Device Manager .....	641
How to Access a Device View .....	642
How to Add or Modify a VLAN .....	643
Adding a VLAN .....	643
Modifying a VLAN .....	643
How to Configure a Bridge Filtering Database .....	645
Configuring Filter Information .....	645
Deleting an Address .....	647
Setting the Age Time .....	647
How to Configure Port Egress State .....	648
How to Find a Source Address .....	649
Device Manager Windows .....	650
Bridge Extension Configuration Window .....	651
Bridge Capability Area .....	651
Bridge Port Capability Area .....	653
Bridge Extension Port GARP Times Window .....	654
Configured Port GARP Times .....	654
Bridge Extension Port GMRP Window .....	656
Port GMRP Information .....	656
Bridge Extension Port Priority Window .....	658



---

Configured Port Priority .....	658
Bridge Extension Port Traffic Class Window .....	660
Configured Port Traffic Class .....	661
Bridge Filtering Database Window .....	663
Source Address Information Area .....	664
Configure Address Filter Area .....	667
Bridge Spanning Tree Configuration Window .....	670
Root Area .....	671
Topology Area .....	672
Configuration Area .....	672
Bridge Port Table .....	673
Bridge Summary Window .....	675
Broadcast Suppression and Statistics Window .....	677
Current Broadcast Suppression Information .....	677
Com Port Configuration Window .....	679
Configuration Upload/Download Window .....	680
Current Device Settings .....	681
Operation .....	682
Download Settings .....	682
Status .....	683
Create/Modify History Window .....	686
Ethernet Port Configuration Window .....	688
Current Port Configuration Information Table .....	688
Configure Parameters .....	690
Auto Negotiate Technology Area .....	691
Find Source Address Window .....	693

---

Firmware Image Download Window .....	695
Current Device Settings .....	696
Operation .....	697
Download Settings .....	697
Status .....	698
ICMP Group Window .....	700
Interface Statistics Window .....	703
Interface Summary Window .....	706
IP Address Table Window .....	708
IP Group Window .....	710
Received Datagrams Area .....	710
Transmitted Datagrams Area .....	711
Datagram Fragments Area .....	712
Datagrams Reassembly Area .....	712
MIB Information Window .....	714
MIBs Tab .....	714
Features Tab .....	714
Net To Media Window .....	716
RMON Alarm/Event List .....	718
Alarms Watch Table .....	719
Events Watch Table .....	720
Create/Modify Alarm Window .....	721
Create/Modify Event Window .....	726
RMON Event Log .....	727
RMON Capture Buffer .....	729
Right-Click Menu .....	729

---

Create/Modify Alarm Window .....	731
RMON Create/Modify Filter Window .....	737
Create/Modify Event Window .....	741
RMON Event Log .....	742
RMON Ethernet Statistics Window .....	744
RMON History Window .....	749
Table View .....	749
Graph View .....	752
RMON History List Window .....	755
RMON Long Term History Window .....	758
Table View .....	758
Graph View .....	761
RMON Long Term History List Window .....	764
RMON Packet Capture .....	767
Right-Click Menu .....	769
SNMP Group Window .....	770
Errors Area .....	771
Totals Area .....	772
System Group Window .....	775
SysORTable .....	776
TCP Group Window .....	778
TCP Connections Information .....	780
UDP Group Window .....	782
Listener Table .....	783
VLAN Configuration Window .....	784
Configured VLANs .....	784

---

Fields and Options .....	785
VLAN Egress Port Configuration Window .....	787
Selected VLAN .....	788
Port Egress Information .....	789
VLAN Port Configuration (Advanced) Window .....	791
Current Port Configuration Information .....	791
Fields and Options .....	793
VLAN Port Configuration (Basic) Window .....	796
Current Port Configuration Information .....	796
Fields and Options .....	798
<b>RoamAbout Wireless Manager Help .....</b>	<b>800</b>
Features and Functionality .....	800
Main Window .....	803
Menu Bar .....	804
File Menu .....	804
Tools Menu .....	804
Help Menu .....	805
Right-click Menu Options .....	805
Toolbar .....	806
Event View .....	806
Right-click Menu Options .....	808
How To Use RoamAbout Wireless Manager .....	809
How to Configure a Device .....	810
How to Create and Apply AP Templates .....	812
Creating a Template .....	812
Editing a Template .....	813

---

Deleting a Template .....	814
Applying a Template to Devices .....	814
How to Monitor AP Statistics .....	815
Packet Statistics Tab .....	815
Line Graph Tools .....	816
Data Table Tab .....	817
Table Tools .....	817
How to Set RoamAbout Wireless Manager Options .....	819
How to View AP Configuration Settings .....	820
AP Interfaces Tab .....	821
AP Interface Security Tab .....	822
AP Clients Tab .....	823
AP Neighbors Tab .....	824
Neighbor Scan Settings Tab .....	824
RADIUS Server Setting Tab .....	825
How to View R2 Configuration Settings .....	827
R2 Wireless Configuration Tab .....	828
R2 Management Information Tab .....	829
R2 Misc Controls Tab .....	829
R2 Error Log Info Tab .....	830

# Extreme Management Center Console Help

---

Console provides unified configuration and control of your wired and wireless network from one or multiple workstations, as well as the sharing of configuration and status information, and common controls and user interface.

Extreme Management Center (Management Center) Wireless Manager, which is included, enables multi-controller configuration management for thousands of access points providing a scalable enterprise wireless management solution.

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

## Management Center Console Features

### Discovery

Discovery populates the Management Center database, discovering devices based on Subnet address or IP range. The discovered devices can be saved to the database, where they are automatically placed in one or more system-created device groups. The system-created device groups sort the devices into appropriate product families, subnets, etc.

### Device Icons, Device Groups, User-defined Groups

In the left tree panel, device icons provide a graphical representation of the device. Device groups appear as folders containing devices. A set of system device groups collect devices by IP, Location, Contact, Chassis, and product families. You can create your own groups organized to show your network in a way that makes sense to you. As an example, you can define a group for a building, or a sub-group within the building as a floor or even another sub-group for a closet. You can create groups based on departments, engineering, sales, etc., or even create groups based on the subnet. The colored indicator next to the device or group icon displays device status as well as the severity of the most severe alarm on the device or in the device group. For more information on alarm/device status indicators, see [How to Configure Alarms](#).

### ExtremeWireless Manager

ExtremeWireless Manager is a tool that enables you to configure and manage multiple ExtremeWireless wireless controllers and their associated

wireless APs. Using the Wireless Manager wizards and configuration tools, you can create a new network configuration or clone an existing one, and apply that same configuration to multiple controllers and APs. Wireless Manager compares the configuration in its deployed templates to the actual configuration of managed controllers. Wireless Manager logs an event and alerts you to any conflicts. You can easily identify and address any conflicts using the Conflict Resolution wizard.

### **Policy Control Console**

PCC is a tool that allows IT to delegate control of network usage to less technical personnel. Using a simple web interface, authorized users such as administrative assistants, department managers, and professors can permit or deny access to the Internet, e-mail, and other network services that might otherwise disrupt a meeting or lecture. The Policy Control Console solution requires the installation of a specialized appliance on your network. The functionality in the Policy Control Console will be limited in the absence of this appliance.

### **FlexViews**

Management Center Console provides pre-defined views of the network devices. These views provide information and configuration capabilities across the entire system. In addition, Management Center Console provides the capabilities to create your own FlexViews or modify and filter those provided with Console. The FlexView tables can be filtered, searched, and sorted, making it possible to view specific network conditions: for example, the top ten instances of an object such as the Highest CRC count on ports or the highest packet transmissions by port.

#### **Graphing, Printing and Exporting**

FlexViews are also capable of presenting information as a pie graph, bar graph, or line graph and printing or exporting information to a file or printer. The exported data is saved in CSV or HTML formats and graphs can be exported as BMP, JPG, PNG or TIFF formatted files.

**FlexView Properties** You can use the FlexView Properties to customize pre-defined views and create your own FlexViews to provide the kind of information you need to manage your network.

### **MIB Tools**

MIB Tools lets you examine the MIBs supported by an active device on your network and change the value of a writable MIB object. You can use the MIB Tools window to contact a device, view its supported MIBs, query the device for MIB values, and set a new value for a MIB object at the device.

## VLAN Tools

The VLAN tools provide a system-wide deployment of VLAN configuration and monitoring capabilities. Use them to create VLAN configuration parameters that are deployed to multiple devices or groups of ports easily and in an automated fashion.

## Basic Policy

The Basic Policy feature lets you view and configure port default policy. You can also use the feature to view information about port login sessions, including authentication type and the role under which the user authenticated.

## Compass

Compass is where you can search for information about end-users or computers. It answers questions such as: Where is this IP address in the network? Where are all members of this IP subnet in the network? Which users are authenticated on this switch, in this building, in the entire network? Where is user Bob Smith logged on currently? Answers to these types of questions help network administrators with information about users and where they are connected. In today's mobile work force it is imperative to be able to find information about users quickly.

## Alarms and Events

The alarms and events feature of Management Center Console can help to make you aware of a variety of situations that demand your attention. The information available from **Alarm and Event** tabs can be exported, printed, searched, filtered, and sorted. Management Center Console also provides configuration tools that let you add and customize **Alarm and Event** tabs and let you trigger e-mail notification or launch an application for certain alarms, events, and traps.

## Device Manager

Provides status and administrative tools to help you manage the devices in your network.

# Document Version

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



---

<b>Date</b>	<b>Revision Number</b>	<b>Description</b>
06-16	7.0 Revision -00	Extreme Management Center 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release
01-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9034979-01

# Console Configuration Considerations

---

Review the following configuration consideration when installing and configuring NetSight Console.

- NetSight Console supports secure command line connections to devices using Secure Shell (SSH). Refer to the specific device user reference manuals for configuration information related to SSH.
- Compass resolves IP addresses to MAC addresses using information from router MIBs (ipNetToMediaTable, ipCidrRouteTable, and ipRouteTable), but only if devices that can be modeled as a switch or a router are created in the NetSight database using the router's IP address. Compass cannot query information from the router MIBs unless devices are created using an IP address for the router interface.
- Policy Control Console's ability to use scripts as a way to set policy is not supported on NetSight Servers installed on a Windows platform system, unless you are using the external PCC appliance.

# Getting Started with NetSight Console

---

Getting Started is a starting point for first-time Console users and for users moving to NetSight Console from NetSight Element Manager. It takes a brief look at Console's features and components and then leads you step-by-step through several tasks that you must perform before you can begin using Console to manage your network. For users coming from Element Manager, Getting Started offers tips to help you find the tools in Console that can be used to perform tasks that you previously performed with Element Manager.

Because Getting Started is meant to be used side-by-side with Console, it is most useful if you install NetSight Console first. Once Console is installed, you can use the steps and suggestions below to begin using some of the features available with Console. When you've finished Getting Started, you will be able to:

- Define user access to Console
- Select Console options.
- Establish device access (Profiles and Credentials)
- Use Discover to add device models to the NetSight database
- Manually add a device
- Monitor alarms and events
- Use Compass to find a device
- Use FlexViews to view device information as a table, pie graph, bar graph, and line graph.

It is recommended that you read the following NetSight Console information in sequence before you implement NetSight Console on your network:

- Installation
- Release Notes
- **Getting Started with NetSight Console** (this guide)

This guide covers three areas:

- [NetSight Console Overview](#)
- [Beginning to Use Console's Features](#)
- [Where to Go from Here](#)

---

---

## Related Information

For information on related topics:

- [NetSight Console Overview](#)
- [Setting Access Privileges](#)
- [Populating the NetSight database](#)
- [Setting Console Options](#)
- [Using Compass to locate a device](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)

# NetSight Console Overview

---

NetSight Console provides a collection of software tools that can help you manage networks of varying complexity. Each is designed to facilitate specific network management tasks while sharing data and providing common controls and a consistent user interface.

## Take a Look Around

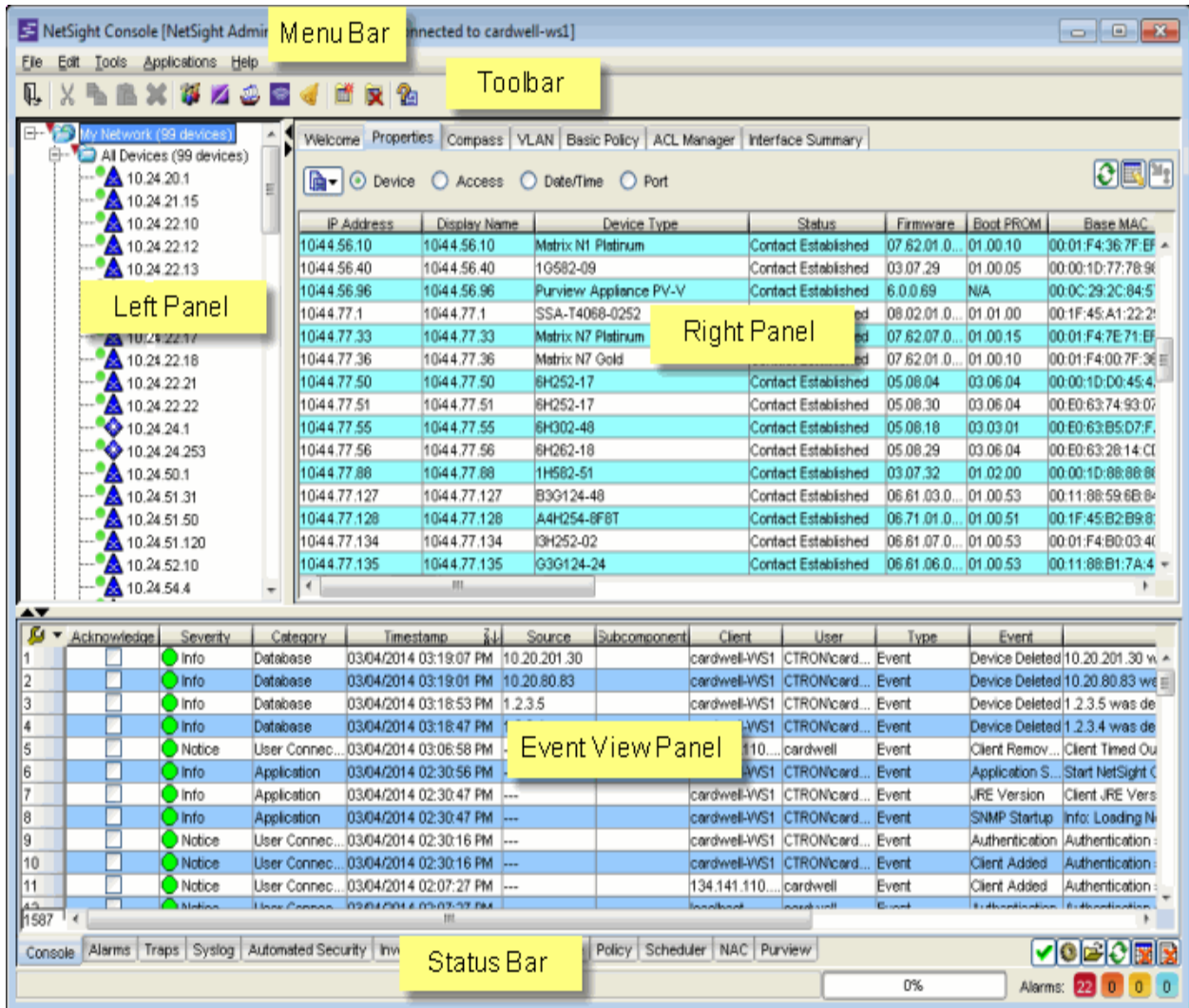
When Console's main window appears, take a few minutes to explore the main window features (toolbar and menus, left and right panel and the Events panel).

In the left panel, expand the **My Network** folder and its sub-folders to see the groupings that are provided with Console. The blue folders are system folders and they cannot be deleted or renamed. You'll be able to add your own folders to the My Network folder when you're ready to create device groups for your network. These user-created groups are tan.

As its name implies, the All Devices folder contains all of the devices that have been created in the database. All of the other folders (the **All Devices** folder, the **All Port Elements** folder, the **Grouped By** folder and its sub-folders, and the folders that you create) let you collectively manage groups of devices. The system groupings are automatically maintained by Console, such that when a new device is added to the database, a copy of the device is placed in the appropriate system group folder. You manage the content of your folders using editing tools from the Edit menu, or from the right click popup menu or by dragging and dropping one or more device from one location to another.

## Main Window

The main window is divided into several functional areas:



## Menus

The menu bar provides access to tools and functions that help you manage your network. Specific menu options are dynamically enabled and disabled depending on which window, object, and tab is selected. The Toolbar and right-click menus provide many of the same options available from the menu bar.

## Toolbar

The Toolbar on the Main Window provides easy access to some of the more commonly used Console functions. The specific Toolbar buttons that may be active depends on your current selection within the Console application. Pausing with your mouse pointer over the toolbar icons displays tool tips showing the button's function.

### *Left (tree) Panel*

The left panel contains the **My Network** folder where you'll find device groups containing the devices that you've discovered and modeled in the NetSight database. In addition to the All Devices group and the All Port Elements group, Console provides groups based on Chassis, Contact, Device Type, IP address, and Location. You can also add your own unique groupings according to the management needs of your network.

### *Right (tabbed) Panel*

The device(s) or device group(s) selected in the left panel determines the specific information that appears in the right panel. The following tabs are available in the right panel:

- [Properties](#) - This tab presents a table of in-depth information about the devices or device groups selected in the left panel. Four radio buttons let you select between Device properties, Access properties, Date/Time, or Port properties. When your user credentials permit, the Table Editor and Enforce features available with many of Console's tables let you edit cell values and perform SNMP sets for certain writable attributes.
- [Compass](#) - This powerful search tool provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations.
- [VLAN](#) - The VLAN tab provides VLAN configuration and monitoring capabilities.
- [Basic Policy](#) - The [Basic Policy Tab \(Default Port Role view\)](#) displays the default policy role configured for each port and lets you change the role, if desired. The [Basic Policy Tab \(End User Sessions view\)](#) displays port end user sessions.
- [ACL Manager](#) - ACL Manager provides the tools that let you efficiently manage the Access Control Lists (ACLs) on your Extreme Networks routers.
- **Interface Summary** and **Diagnostic Messages** - These tabs present default [FlexViews](#) that shows basic interface information (speed, IP Address, type of interface) and diagnostic information for the current left panel selections. FlexViews present information in several formats (table, pie graph, bar graph, and line graph) and allow you to filter the table information and export the information to formats that are compatible with other business applications.

Console provides a FlexView editing capability that lets you modify existing FlexViews and create new ones to serve your need for information.

### *Event View Panel*

NetSight Console's Event View tables let you view alarm, event, and trap information for the NetSight Console, network devices, and other NetSight applications. Each tabbed view lets you scroll through the most recent 50,000 entries in the logs that are configured for that view. A **Console** tab showing Console events, an **Alarms** tab showing information about current network alarms, and a **Traps** tab that captures traps from devices modeled in the NetSight database, are provided when NetSight Console is initially installed. The **Syslog** tab shows events from devices that are configured to use the NetSight Syslog Server. You can add your own tabs that allow you to monitor events generated by NetSight applications and alarms and traps from network devices.

### *Status Bar*

Operational information is available here as text messages and a progress gauge.

---

## **Related Information**

For information on related topics:

- [Setting Access Privileges](#)
- [Setting Console Options](#)
- [Populating the NetSight database](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)



## Beginning To Use Console's Features

---

This section contains **Getting Started** topics that can help you to start using the features provided with NetSight Console.

- Setting Console Options
- Setting Access Privileges
  - Define user access to Console
  - Establish device access (Profiles and Credentials)
- Populating the database
  - Use Discover to add device models to the NetSight database
  - Manually add a device
- Use Compass to find a device
- Monitor events and alarms
- Use FlexViews to view device information as a table, pie graph, bar graph, and line graph.

## Setting Console Options

---

You can customize many of Console's features to suit your needs or the needs of your network using Console options. These options are available from the Options window (**Tools > Options**).

We'll set the **Discover** option to familiarize you with the Console options. After that, you can refer to [How to set Console Options](#) to customize other options to suit your needs.

To open the Options window:

1. Select **Tools > Options** from the menu bar. The Options window opens.
2. **Set Console's Discover Options:**  
These options apply only to the NetSight Console application.
  - a. Set the **Number of SNMP Retries**. This is the number of attempts that will be made to contact a device when an attempt at contact fails. 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 SNMP Timeout** field, enter the amount of time (in seconds) that Discover waits before re-trying to contact a device.

**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. The default setting for Discover is 500.
- d. In the Table Colors section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.

3. Click **OK** to set the options and close the window.
- 

## Related Information

For information on related topics:

- [NetSight Console Overview](#)
- [Setting Access Privileges](#)
- [Populating the NetSight database](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)

## Setting Access Privileges

---

Among the first things that should be done when you begin using Console is to establish access privileges. These fall into two major categories: access to Console and other Extreme Management Center applications, and access to the devices on your network.

### *Defining User Access to Extreme Management Center*

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 Management Center client or access the Management Center database using the Management Center Server Administration web page. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

In addition to configuring the authentication method, you must also create the authorization groups that define the access privileges (called *Capabilities*) that will be 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.

When you install Management Center, the user performing the installation is created as an Authorized User with Management Center Administrator capabilities. This administrative user is capable of creating additional Management Center users and assigning their access levels. For complete steps in configuring authentication methods and creating authorization groups, see *How to Configure User Access to Extreme Management Center Applications* under Authorization/Device Access in the Suite-Wide Tools user guide.

In addition to defining user access to Console, you can define user credentials and profiles to control access to the devices on your network.

### *Establishing Device Access (Credentials and Profiles)*

Establishing access to the devices on your network from Console depends on creating identities that Console can use for authentication when performing SNMP queries and sets. Console supports authentication to devices using SNMPv1, SNMPv2 and SNMPv3. When device models are created in the Management Center database, you can accept the *default* profile or assign a specific *Profile* to describe a set of access *Credentials* that Console will use for authentication at each level of access in the device. (When first installed, Console's default profile uses an SNMPv1 credential that provides Read, Write and Max Access privileges.) The specific profile that is used depends on the protocol that is supported in a device and the credentials that are required to be granted access.

#### **SNMPv1 or SNMPv2**

For SNMPv1 or SNMPv2, authentication consists of providing the correct community name for a particular access level (Read, Write and Max Access). As long as device models in Console are assigned a Profile with the correct community names, access is granted.

### SNMPv3

Establishing contact with SNMPv3 is somewhat more complex. SNMPv3 uses a User-based Security Model (USM). Before access is granted to a particular level, a security user (in this case Console) and a set of authentication and privacy keys must be verified by the device's SNMP engine. These are defined as a **Credential**, which are then linked to a Profile that Console will use when contacting a device.

Configuring device access consists of first creating credentials and then creating the profiles that will use those credentials. For complete instructions, see How to Configure Profiles and Credentials under Authorization/Device Access in the Suite-Wide Tools user guide.

---

### Related Information

For information on related topics:

- [Console Overview](#)
- [Setting Console Options](#)
- [Populating the Extreme Management Center database](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)

## Populating the NetSight Database

---

The NetSight database contains device models that represent the actual devices on your network. The models store attributes for your devices and make it possible to maintain an array of access levels and present status in Console's


views. Console provides three methods for populating the database with device models.

- Discovery, using IP Range or CDP Seed IP discovery
  - **IP Range Discover** -- performs a discover based on one or more IP address ranges. An IP Range Discover discovers all devices within the specified IP address range(s). The steps below will get you started by performing an IP Range discovery.
  - **CDP Seed IP Discover** -- performs a single discover of all CDP-compliant devices in the network, starting with a CDP seed device. To learn more about CDP Seed IP discovery, refer to the [CDP Seed IP Discover](#) section in **How to Discover Devices** help topic.
- [Manually adding device models](#)
- Import from a file - refer to [How to Export/Import a Device List](#) for more information on this method.

### *Discovering Devices*

Discovery lets you to discover the physical elements (devices) of your network, and add them to the NetSight database. You can perform a discover on a specified range of IP addresses, or perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices. Discover automatically explores a specific network segment and creates a list of discovered devices. You can then save the all or a subset of the discovered devices to the NetSight database. Devices that are added to the database are automatically placed in the appropriate groups in the left panel of the main window.

Here's how to do an IP Range Discovery. Begin by opening the Discover window:

1. Select **Tools > Discover** from the menu bar or click the Discover button  in the toolbar. The Discover window opens.

Deciding what type of discovery to use depends on your specific network configuration. Generally, if your network has all CDP-compliant devices that are configured with the same SNMP access parameters, the CDP Seed IP Discover is recommended. If your network has no CDP-compliant devices, or a mix of CDP and non-CDP-compliant devices, the IP Range Discover is recommended.

2. Select the **IP Range tab**.

At the top of the tab is a table where you specify the IP address ranges. Each row defines a single range. When you first open the tab, a default range is displayed based on the IP address of the Console workstation. You can edit this row to specify a different range and add new rows to specify additional discovery ranges.

3. To add a new range, right-click on an existing row and select **Insert Row**. A copy of the selected row is added as a new row immediately above it. (Tabbing past the last row also adds a new row to the end of the table.)

The position of a row determines the range's **Precedence**, as indicated in the second column. Precedence determines which parameters will be used if a device is in more than one range (the lower number yields higher precedence). For example, if a device is in two ranges -- one range with a precedence of 1 using an SNMPv3 profile, and the other range with a precedence of 2 using an SNMPv1 profile -- the device will be saved with the SNMPv3 profile because that range has the higher precedence.

4. To edit a range, simply tab through the parameters and either enter a new value or use the drop-down list to select a value.
  - a. **Enabled** - Select the checkbox to enable Discover for this IP address range. Only enabled ranges are searched when a discover operation is performed.
  - b. **Start IP** - Enter the IP address at which the range should begin.
  - c. **End IP** - Enter the IP address at which the range should end.
  - d. **Profile** - Use the drop-down list to select the access Profile that will give the Discover tool read access to the devices you wish to discover. This list contains a default profile, all of the profiles that you've created and a **Ping Only** choice. Ping Only allows discovering devices, such as workstations and other devices that are not configured for SNMP. If Ping Only is selected, the Poll Type must be set to **Ping**. Click the **Profile Details** button to open the Authorization Configuration/Device Access Window - Profiles/Credentials Tab where you can create and edit Console profiles. If you discover an existing device using a different profile than the device is already using in the database, saving the device will overwrite the profile currently being used in the database.
  - e. **Poll Type** - Use the drop-down list to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified,

the SNMP version (SNMPv1, SNMPv2, or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. If you discover an existing device using a different poll type than the device is already using in the database, saving the device will overwrite the poll type currently being used in the database.

---

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

---

- f. **Poll Group** -- Use the drop-down list to select a Poll Group for the discovered devices. Console provides three distinct poll groups (defined in the Status Polling view of the Suite-wide Options window) that each specify a unique poll frequency. When you save newly discovered devices to the database, they will be polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.
- 

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

---

- g. **Vendor** -- Use the drop-down list to specify whether you want to discover all devices or only Extreme devices.

5. Click **Discover** to begin the discover operation. Discovered devices are listed in the [Discovered Devices table](#). The progress of each range discover is displayed as a percentage in the corresponding Progress column.
- 

**NOTE:** When a Discover operation is initiated, all rows (including Disabled rows) are checked for validity. If any rows have invalid parameters, the Discover will not be performed. An error message will alert you to the invalid entry, which must be corrected or deleted before the Discover operation can be performed.

---

6. After the discover is complete, click **Save All** to save all the discovered devices to the NetSight database, or select the desired devices in the Discovered Devices table and click **Save** to save those devices to the database. To remove a device from the table, select the device and click **Remove**.

**NOTE:** If the IP Range includes broadcast addresses (.0, .255, .127, .128, depending on the subnet mask), the addresses may be discovered as "devices". To make the polling of devices in the Console tree as efficient as possible, these addresses should be removed and not saved to the database.

It is recommended that you backup the NetSight database (**File > Database > Backup**) after you have saved your discovered devices.

7. To delete an IP range, right-click on the table row and select Delete Row. You can select and delete multiple rows.

---

**TIP:** Specify as narrow an IP address range as possible. The wider the range, the longer it will take to perform the discover. For example, if you are discovering IP addresses 111.111.111.20 through 30, and 111.111.111.240 through 250, it is faster to create two separate discovers for each range rather than performing one discover for 111.111.111.20 through 250.

---

### *Adding Devices Manually*

You can manually add individual device models to the NetSight database:

1. Click the right mouse button on the group to which you want to add a device and select **Add Device** from the right-click menu. The **Add Device** window opens, where you can define the IP address and Profile for the device being added.
2. Type an **IP Address**.
3. Use the **Profile** drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.
4. You can use the default nickname or click **Specify** to assign a unique nickname to this device. The default nickname for SNMP devices is the *sysName* MIB object, or if no *sysName* has been assigned, the device's IP address. The default nickname for pingable devices is the IP address.
5. Click **Apply**. The new device appears in the group and is automatically added to the **All Devices** group.

---

### **Related Information**

For information on related topics:



- [NetSight Console Overview](#)
- [Setting Console Options](#)
- [Setting Access Privileges](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)

---

## Using Compass

Compass is a powerful search tool that provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations. You can use Compass to search one or more devices or device groups selected in the Console left panel. (If you do a search on a user-created group that contains interfaces, the whole device on which the interface is located will be searched.) The search is based on the following:

- the selection you make in the Console left panel ([Search Scope](#))
- the [Search Type](#) you select on the Compass tab
- the [Search Parameters](#) you provide on the Compass tab

We'll use Compass to find a device to demonstrate how to use Compass, but that is just one of its many capabilities. Refer to [How to Use Compass](#) to learn how to use all of Compass' features. To find a device:

1. Click the Compass tab in the right panel of the main window.
2. In the left panel, select the device group(s) or device(s) that you want to search.
3. Select the Compass tab in the right panel.
4. Select Auto from the Search Type drop-down list.
5. In the Address text field, enter an address or hostname, using any of the allowed [formats](#).
6. Select any desired [Results Filters](#) (you can also do this after the search is completed).
7. Click **Search**.

8. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
  9. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.
- 

## Related Information

For information on related topics:


- [NetSight Console Overview](#)
- [Setting Console Options](#)
- [Setting Access Privileges](#)
- [Populating the NetSight Database](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)

## Monitoring Alarms and Events

---

The NetSight Event View (located at the bottom of the NetSight Console main window) lets you view alarm, event, and trap information for Console and other NetSight applications. There are four Event View tabs when Console is first installed: Console, Alarms, Traps, and Syslog. In addition, there are tabs for each NetSight application you have installed.

You can use the Event View Manager (Tools > Alarm/Event > Event View Manager) to add additional event logs to suit your needs and use the Alarms Manager (Tools > Alarm/Event > Alarms Manager) to configure network alarms that provide status information for a particular problem on a particular network device. Refer to [How to Configure Alarms](#) for more information on configuring network alarms.

Each tabbed view in the Event View lets you scroll through the most recent 10,000 entries in the logs that are configured for that view. By default the table is sorted chronologically using the entries in the **Date/Time** column, with the most recent entry in the top row. You can check the Acknowledge column to mark entries that you've viewed, then click the  to hide the rows containing

acknowledged events and traps. Each table's right-click menu provides options to hide or show multiple rows with a single operation.

---

### **Related Information**

For information on related topics:



- [NetSight Console Overview](#)
- [Setting Console Options](#)
- [Setting Access Privileges](#)
- [Populating the NetSight database](#)
- [Using Compass to locate a device](#)
- [Working with FlexViews](#)
- [Where to Go from Here](#)


## Working with FlexViews

---

Console comes with a set of FlexViews that lets you view a wide variety of information about the devices on your network as a table, bar graph, line graph, or pie chart. When NetSight Console is initially installed, the Interface Summary is the default FlexView, accessible from the **Interface Summary** tab in the right panel. It's a good place to start using FlexViews.

To begin using FlexViews, we'll select a single device and take a look at the information that it returns:



1. Select a device in the left panel (choose a device, such as a router, where there is traffic). FlexViews always present information about your selection in the left panel.
2. Click the Interface Summary tab in the right panel.
3. Click the  button on the FlexView toolbar and select **Open** from the menu. A file browser opens to the FlexViews folder. This is where all of the FlexViews that come with Console are stored. To see a catalog of all these FlexViews, refer to [How to Export a FlexView Catalog](#).
4. Navigate into the `Interface` folder and open the `Interface Statistics.tpl` file.
5. Set the **Poll Frequency** to 0 and click  (Retrieve). This forces a single poll cycle to retrieve information from the selected device.

The Retrieve button changes to a  (Stop button) and the progress of the poll is reported on the Console's [Status](#) bar. The table fills with the information returned from the device and when the polling is completed, the button returns to a Retrieve button.

You can click on column headings to sort the table using the information from a column. You can right click anywhere in the table body to choose from several options on the popup menu. Refer to Right-Click Menus in the FlexView help topic to learn more about right-click menu options.


6. Click the **In\_Octets** column heading twice. The first click sorts the column in ascending order, the second sorts the column in descending order. If there is no traffic, as indicated by the In\_Octets values, select and poll another device until you find one that shows some traffic.


### Viewing the table information as a pie graph or bar graph

7. With the FlexView containing your device information, click  (Pie Graph). A Pie graph, is displayed above the table information in the left panel. The additional controls for the graph are available from the tabbed panel at the right of the window. The center panel is a legend showing the current graph selections.
8. Click the **Columns** tab and check In Octets and Out Octets. The graph content reflects the contribution to the pie from In Octets and Out Octets.
9. Click the **General Controls** tab. The content of this tab changes, depending on whether you've selected one column or multiple columns. With multiple columns selected, the pie can show you the minimum, average, or maximum values for each of the selected columns. When only one column is selected, you can display several rows in the pie, showing the contribution from each row as a slice in the pie. If you hover over a particular slice in the pie, a tool tip is displayed with the value for that slice.
10. Now, click  (Bar Graph). The view changes to show the values from the same two columns, each as a separate bar.

Both Pie and Bar graphs provide a snapshot of the values at a given point in time. A line graph on the other hand, can show you how specific values change over time.

### Viewing the table information as a line graph

11. Set the Poll Frequency to 5 (seconds). Once, you click Retrieve, Console automatically start retrieving information from your left panel selection at the specified interval.
12. Click  (Line Graph). A blank Line graph is added above the table and a **Graph Data** tab is added to the table information in the bottom panel. Also, the **Line Graph Controls** tab is now active in the tabbed panel at the right of the window. The center panel is a legend showing the current graph selections.
13. Adjust the pane sizes to allow viewing the entire graph and access to tabbed panel settings.
14. Click the **Columns** tab and check only **In Octets**.
15. Click the **General Controls** tab, select **Highest** and set the number of rows to sample to 3. (The selection of the highest rows to be plotted is determined by the values returned from the first query.) Leave the other settings blank for now. This should let you explore the graph operation without too many plots.

16. Click the **Line Graph Controls** tab and set:
  - **Graph Type** - Delta
  - **Graph 5 Samples**
  - Check **Moving Avg - Samples** and set the samples to 3.
  - Leave the remaining settings unchecked.
17. Click **Retrieve**. The Retrieve button changes to  and the FlexView begins polling at the specified Poll Frequency and plotting three lines, one for each of the three highest values.

A (blank) gap in a line indicates that there was no response from the device for that poll and no point was plotted. Dashed lines begin plotting the **Moving Averages** with the third poll cycle. The polling will continue until the Retrieve button is clicked to stop polling.

---

## Related Information

For information on related topics:

- [NetSight Console Overview](#)
- [Setting Console Options](#)
- [Setting Access Privileges](#)
- [Populating the NetSight Database](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Where to Go from Here](#)

## Where to Go from Here

---

At this point, you've tried many of Console's features and need only expand your knowledge and develop techniques for using them on your network. Console's **VLAN** management is the only area that has not been touched by Getting Started. To learn more about VLANs, begin by reading the VLAN concepts information, available from Console Help. Help is also the source for a variety of conceptual and task-oriented topics.

### Accessing NetSight Console Help

All Console documentation is available in the Help system accessible from the application.

- Help on Console features is available via the **Help > Help Topics** menu option.
- Help for the tab currently displayed in the right panel is available via the **Help > About This Window** menu option (or from the Help button on the main toolbar).
- Help for a particular window is also often available via a **Help** button on the window itself.

Any time you access Help, you can navigate to any other file in the Help system. There is also a Search feature within the Help.

1. Select **Help > Help Topics** from the menu bar. The NetSight online Help opens in a browser window. A Table of Contents in the left panel displays the available topics in the NetSight Help.
2. Close the Help window.
3. Notice what tab is currently displayed in the right panel of the Console window, then click the Help button on the toolbar (or select **Help > About This Window** from the menu bar). The online Help opens with specific information about the particular tab, and all aspects of the Help system are still available.
4. Close the Help window.
5. In the Console left panel, select the **All Devices** device group, then right-click on the folder and select **Add Device**.

6. Click the **Help** button in the Add Device window. Specific information about the window is displayed, and all aspects of the Help system are still available.
7. Click the **Search** (magnifying glass) accordion tab at the bottom of the left panel of the Help window to open the Search panel. Enter a term you are searching for in the search field and then click **Search**. A list of topics containing the term appears in the Search panel ranked according to the number of times the term appears. You can refine the Search results by using the Filters drop-down menu to select which NetSight application you are interested in searching. If you want to find a specific combination of words that are always next to each other in the same order (e.g., domain name), you can enter the search keywords within quotation marks (e.g., "domain name").

---

**NOTE:** You can also use the Quick search field in the Help toolbar to search for a term on the current page.

---

## Related Information

For information on related topics:

- [NetSight Console Overview](#)
- [Setting Console Options](#)
- [Setting Access Privileges](#)
- [Populating the NetSight database](#)
- [Using Compass to locate a device](#)
- [Monitoring Alarms and Events](#)
- [Working with FlexViews](#)



# NetSight Console Concepts

---

The **Concepts** help section contains help topics that can help you understand how NetSight Console works and help you get started using Console.

# VLAN Concepts

---

The following concepts will assist you in configuring VLAN and port template definitions for your VLAN models in NetSight Console.

Information on:

- [Egress Rules \(Transmitting Frames\)](#)
  - [Dynamic Egress](#)
    - [GVRP](#)
    - [GARP Timers](#)
- [Enforcing](#)
- [Frame Types](#)
- [IGMP](#)
  - [Interface Robustness \(Robustness Variable\)](#)
  - [Last Member Query Interval](#)
  - [Query Interval](#)
  - [Query Response](#)
- [Ingress Filtering](#)
- [Priority Classification](#)
  - [Weighted Priority](#)
- [Verifying](#)
- [VLAN Identification](#)
  - [Port VLAN ID \(PVID\)](#)
  - [VLAN ID \(VID\)](#)
- [VLAN Model](#)
- [VLAN Learning](#)

## Egress Rules (Transmitting Frames)

A device determines which frames can be transmitted out a port based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether

the frames will be transmitted as tagged or untagged frames. You can add or remove ports to or from a VLAN's Egress List, thereby controlling which VLAN's frames can be forwarded out which ports.

When a frame is transmitted out a port, the device first checks the Egress List. If the port is listed on the Egress List of the VLAN associated with it, the frame is then transmitted according to the priority assigned to the frame. The frame is transmitted as tagged or untagged according to the specification in the Egress List. If the port is not on the Egress List, or if the port is not operational, the frame is discarded.

### *Dynamic Egress*

In NetSight Console, you can control whether or not Dynamic Egress is enabled for a VLAN in the VLAN [Definitions view](#). When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means that you do not need to add the ingress port to the VLAN's egress list manually. (See [Example 1](#), below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. In the [Port Template Definitions view](#), you can enable [GVRP](#) (GARP VLAN Registration Protocol), which automatically adds the interswitch ingress ports to the egress lists of VLANs. (See [Example 2](#), below.)

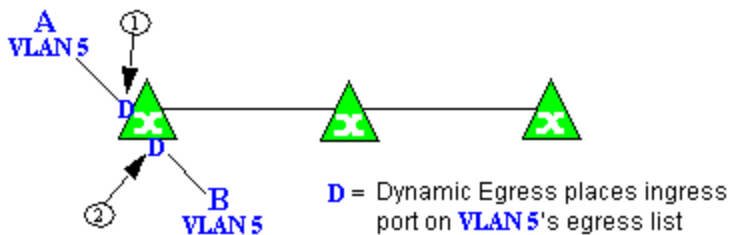
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See [Example 3](#), below.)

If an endstation is talking to a "silent" endstation which does send responses, like a printer, you will need to add the silent endstation's ingress port to the VLAN's egress list manually with a tool like NetSight Device Manager, or local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See [Example 4](#), below.)

**CAUTION:** If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries will time out. The result is that an endstation will appear "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A & B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A will not be able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

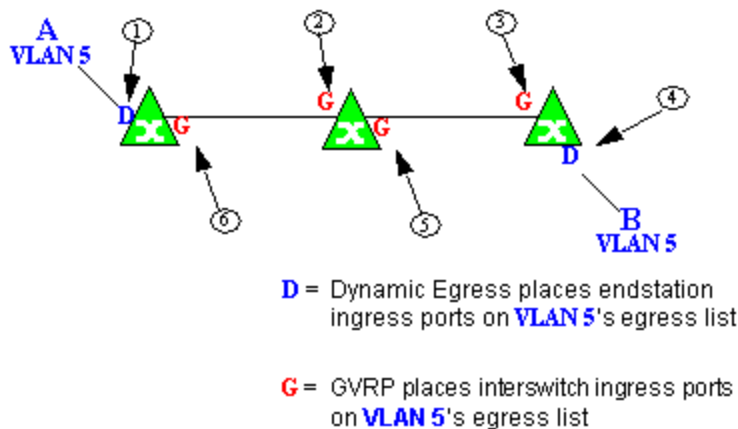
### Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.



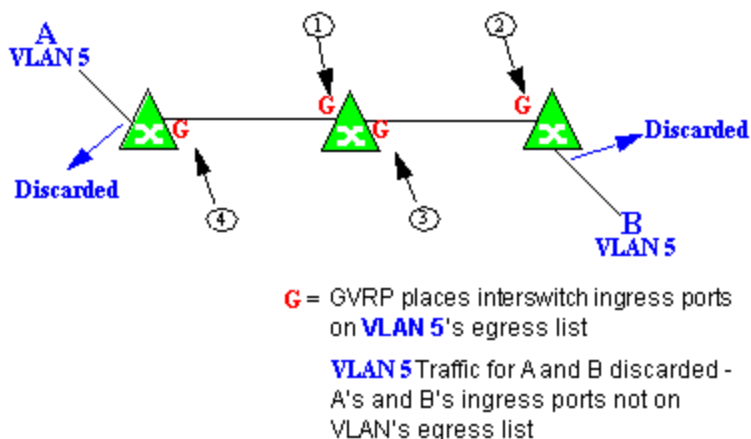
### Example 2: Dynamic Egress + GVRP

In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (4) on VLAN 5's egress list. GVRP then places interswitch ingress ports (5) and (6) on VLAN 5's egress list. The devices can then forward traffic to both endstations.



### Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.



### Example 4: Silent Endstation

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

ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.

## GVRP

GVRP (GARP VLAN Registration Protocol) dynamically adds interswitch ingress ports to the egress lists of VLANs across a domain. You can enable and disable GVRP in the [Port Template Definitions](#) view.

---

**NOTE:** If you do not want GVRP enabled on your network, you can disable it, then manually configure the interswitch ports to do what GVRP does automatically, using MIB Tools or local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration.



---

## GARP Timers

In the [Port Template Definitions](#) view, you can set GARP timers on the device to control the timing of dynamic VLAN membership updates to connected devices. The timer values must be identical on all connected devices in order for GVRP to operate successfully.

- **Join Time** - Frequency of messages issued when a new port has been added to the VLAN. Possible values are 1 through 1488800 milliseconds.
- **Leave Time** - Frequency of messages issued when a single port no longer belongs to the VLAN. This value must be at least three times greater than the Join Time. Possible values are 1 through 1488800 milliseconds.
- **Leave All Time** - Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. This value must be greater than the value for Leave Time. Possible values are 1 through 1488800 milliseconds.

## Enforcing

When working with VLANs in NetSight Console, you can write the definitions in the VLAN model to selected devices or ports by clicking the **Enforce** button  on the [Device](#) or [Advanced Port](#) view of the right panel VLAN tab in Console's main window. You can also enforce changes to individual ports on the Basic Port view of the VLAN tab in Console's main window. A green exclamation point  in a table indicates that the setting will be written to the device when you

[enforce](#). Only those VLANs which have the [Write VLAN to Devices](#) box checked on the VLAN Properties tab are enforced. A [verification](#) is done automatically after the enforce is complete. A red **✘** appears if the enforcing of a particular setting fails.

---

**NOTE:** On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS\_L3\_Interface Name). However, you can [update](#) a VLAN model definition with the System Static VLAN definition from the router.

---

## Frame Types

Incoming frames are processed according to ingress rules which determine the VLAN membership and transmission priority of a frame received on a port by checking for the presence of a VLAN tag. A VLAN tag is a field within a frame that identifies the frame's VLAN membership and priority.

Frames can be tagged or untagged. A tagged frame is a frame that contains a VLAN tag. An untagged frame does not have a VLAN tag, but will be tagged when it is received on a port. A tagged frame may have already been processed by an 802.1Q switch or originated at an endpoint capable of inserting a VLAN tag into a frame. A VLAN tag may or may not contain a VLAN ID (VID), but it will always contain priority information. End systems are allowed to transmit frames with only a priority in the VLAN tag. When switches transmit a tagged frame, the VLAN tag will always include a VID along with the priority.

Tagged and untagged frames are assigned VLAN membership and transmission priority differently:

### Untagged Frame - VLAN Membership

When an untagged frame is received on a port, if a VLAN Classification rule exists for the frame's classification type, the frame will gain membership in the associated VLAN. If not, the frame will be assigned to the VLAN identified as the port's VLAN ID (PVID).

### Untagged Frame - Priority Assignment

When an untagged frame is received on a port, if a Priority Classification rule exists for the frame's classification type, the frame will be assigned the associated priority. If not, the frame will be assigned the port's default priority.

### Tagged Frame - VLAN Membership

If a tagged frame includes a VID (VLAN ID), it will gain membership in the VLAN indicated by the VID. If not, and a VLAN Classification rule exists for the frame's classification type, the frame will be put into the associated VLAN. If there is no VID or classification rule, the frame will be put in the VLAN associated with the port's VLAN ID (PVID).

### Tagged Frame - Priority Assignment

When a tagged frame is received on a port, it is assigned the priority contained in the VLAN tag.

You can set the acceptable frame type for a port on the [Port Template Definitions](#) view.

## IGMP

IGMP (Internet Group Management Protocol) is a protocol used by IP hosts and their immediate neighbor multicast agents to support the allocation of temporary group addresses and the addition and deletion of members of a VLAN. You can enable and disable IGMP on the [VLAN Definitions](#) view.

### *IGMP Intervals*

You can control the following IGMP query settings on the [VLAN Definitions](#) view:

- **Query Interval** - Interval (in seconds) between general IGMP queries sent by the device to solicit VLAN membership information from other devices. By setting this interval, you can control the number of IGMP messages on a subnet. Larger values cause queries to be sent less often. The Query Interval must be greater than the Query Response interval. Valid values: 1 through 300 seconds.
- **Query Response** - Maximum amount of time allowed for responses to general IGMP queries. By setting this value, you can control the burstiness of IGMP messages on a subnet. Larger values result in less bursty traffic, because host responses are spread over a larger interval. This value must be less than the Query Interval. Valid values: 1 through 300.
- **Interface Robustness (Robustness Variable)** - Indicates the susceptibility of the subnet to lost packets. If a subnet is particularly susceptible to losses, you may wish to increase this value. IGMP is robust to (Robustness Variable-1) packet losses. The Interface Robustness value is used in the calculation of IGMP message intervals. Valid values are 2 thru 32767.



- **Last Member Query Interval** - Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. By setting this value, you can control the "leave latency" of the network. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds.

## Ingress Filtering

Ingress Filtering is a means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame. For example, if a tagged frame with membership in the Sales VLAN is received on a Port 1, and Ingress Filtering is enabled, the switch will determine if the port is on the Sales VLAN's Egress List. If it is, the frame can be processed. If it is not, the frame is dropped. You can set ingress filtering for a VLAN on the [Port Template Definitions](#) view.

## Priority Classification

Priority Classification is used to assign frames transmission priority over other frames. Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority.

Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

Frames can be assigned a transmission priority ;based on the default priority of the receiving switch port, regardless of the frame's classification type. However, with the addition of classification rules, frames can be assigned a priority based on the frame's classification type. Using priority classification rules, network administrators can classify a frame based on Layer 2/3/4 information to have higher or lower priority than other frames on a per port basis, allowing for better defined Class of Service configurations.

You can set the default priority for incoming frames on the [Port Template Definitions](#) view.

## *Weighted Priority*



Weighted priority, available on certain devices, is a way to further refine [priority classification](#). You can control this setting on the [Port Template Definitions](#) view.

Some devices support four transmit queues (0-3) per port. These queues can be serviced based on a strict method, meaning that all frames in Queue 3 will be transmitted before the frames in Queue 0, or based on a fair weighted method. The weighted method allows the network administrator to give a certain percentage or weight to each queue, preventing a lower priority queue from being starved.

Forwarding priority can be tuned to allocate a percentage of a port's transmit resources to the each traffic queue. This lets you adjust a strict priority scheme to guarantee that some percentage of frames from lower priority queues will always be sent. Weighted priority settings divide each port's transmit resources into 16 equal parts, which can be allocated to traffic queues in increments of 6.25% (1/16th). The total resource allocation for a port must always add up to 100%.

To understand the effect of weighted priorities, consider a device port with strict priority settings. In this case, all of the frames from the highest priority traffic queue are sent before frames are sent from any of the lower priority queues. Now, assuming four traffic queues, assign weighted priorities for the port giving 50% of the transmit resources to Queue 3, 25% to Queue 2, and 25% to Queue 1 and 0% to Queue 0. With these settings, at least 50% of the frames will be transmitted from Queue 3, at least 25% from Queue 2, at least 25% from Queue 1 and frames will only be transmitted from Queue 0 when Queue 1, 2, and 3 are empty.

## Verifying

Verifying retrieves the VLAN settings on the selected devices and compares them with the settings in the selected [VLAN Definitions](#) view or [Port Template Definitions](#) view. This is done by way of the **Start Verify (Retrieve)** button  on the [Device](#) or [Advanced Port](#) view of the VLAN tab in Console's main window. (In the [Basic Port](#) view of the VLAN tab in Console's main window, the  button simply retrieves port VLAN information from the selected devices to populate the table.)

Only those VLANs which have the [Write VLAN to Devices](#) box checked on the VLAN Definitions view are compared. Differences are indicated by a red not-

equals symbol **≠** in the device or ports table on the VLAN tab in Console's main window. A green exclamation point **!** is displayed when you select a **≠** line in the table to the model setting that will be written to the device when you [enforce](#). You can review the differences and make modifications to your model as needed, including updating the definitions in your model using the definitions from the selected devices (for VLAN Definitions) or ports (for Port Template Definitions).

For more information, see [How to Work with VLAN Models](#).

## VLAN Identification

VLAN identifiers include VLAN ID's and Port VLAN ID's.

### *VLAN ID (VID)*

802.1Q VLANs are defined by VLAN IDs (VIDs) and VLAN names.

#### **VID**

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

#### **VLAN Name**

An alphanumeric name associated with a VLAN ID, used to make VLANs easier to identify and remember (up to 64 characters).

### *PVID (Port VLAN ID)*

You can change a port's VLAN membership to reflect the specific needs of your network by assigning new VLAN membership to the port. When you assign VLAN membership to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port and the port is added to the VLAN's Egress List.

#### **PVID**

The PVID (Port VLAN ID) represents a port's VLAN assignment. Possible values are 1 through 4094.

#### **Egress List**

The Egress List specifies which ports can transmit the frames associated with the VLAN.

---

**NOTE:** On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

---

## VLAN Model

NetSight Console enables you to create VLAN models and enforce them across multiple network devices. A VLAN model consists of at least one VLAN Definition and one VLAN Port Template, which you can define on the [VLAN Definitions](#) view and the [Port Template Definitions](#) view.

NetSight Console provides you with one VLAN model (the Primary VLAN Model) which is pre-populated with a Default VLAN (VID 1). You can further define this VLAN model, and/or you can create other VLAN models. (The Default VLAN for a model cannot be deleted.)

Once a VLAN model has been created, you can utilize it in the following ways:

- Use the [Basic Port View](#) of the VLAN tab in Console's main window to enforce the properties of a port template on selected devices. You can also make custom edits for selected ports using this view of the VLAN tab in Console's main window.
- Use the [Device](#) or [Advanced Port](#) view of the VLAN tab in Console's main window to perform a more detailed analysis of the differences between the definitions in the VLAN model and the VLAN settings on selected devices and their ports. Using these views of the VLAN tab in Console's main window, you can review the differences and make modifications to your VLAN model and/or device or port VLAN configuration as required, including updating any or all of the definitions in the model with the settings on selected devices and their ports, and writing ([enforcing](#)) a model's VLAN definitions and/or VLAN port templates to selected devices or ports.

See [How to Work with VLAN Models](#) for more information.

## VLAN Learning

VLAN learning allows the creation of groups of VLANs that will share Filtered Database information (MAC address, port, and VLAN ID) according to 802.1Q Shared Learning Constraints (IEEE Std 802.1Q-1998). This helps to speed MAC to port lookups and reduce flooding, because MAC addresses will be in the same Filtering Database.

## Traps and Informs

---

This Help topic provides information about SNMPv3 Notification messages (Traps and Informs). SNMP Notification messages provide the mechanism for one SNMP application to notify another SNMP application that something has occurred or been noticed. The SNMPv3 protocol mandates that all notification messages be rejected unless the SNMPv3 user sending the notification already exists in the remote SNMP agent's user database. The user database in an SNMPv3 application is actually referenced by a combination of the user's name (Security Name) and an identifier for the given SNMP application (Engine ID).

The [snmptrapd tab](#) in the Trap Receiver Configuration window lets you configure the Security User credentials and/or Engine IDs for devices from which the NetSight SNMP Trap Service (snmptrapd) will accept SNMPv3 Notification messages. If this information is not provided as part of the SNMP Trap Service configuration, all SNMPv3 Notification messages are dropped by the SNMP Trap Service. They do not appear in the Console's Event log and they are not acknowledged by the SNMP Trap Service.

SNMPv3 traps and SNMPv3 inform messages differ in operation. When two SNMP agents communicate, one agent is always designated as *authoritative*. This *authoritative* designation depends on the type of message. When an SNMP message expects a response (e.g., SNMPv3 Inform), then the receiver is authoritative. When an SNMP message does not expect a response (e.g., SNMPv3 Trap), then the sender is authoritative. This is important because it is the authoritative agent's Engine ID together with a Security User Name that must be recognized before the receiver will accept the message.

### SNMPv3 Traps

**Traps** are *one-way* notification messages. They are not acknowledged by a receiving SNMP application. The Security User and Engine ID of the sending agent is included in SNMPv3 trap messages. So, before trap messages can be received in Console, the SNMP Trap Service needs to know both the Security User credentials and the engine ID of the sending SNMP agent.

Because of this, you must define the Security User credentials and Engine ID of the SNMP agents for every device from which you want to receive SNMPv3 traps. This information is defined using the `createUser` directive in the `snmptrapd.conf` file. So, if you want to have 100 SNMP agents send SNMPv3

traps to the SNMP Trap Service, you need 100 `createUser` directives (defining both the Security User credentials and Engine IDs) in the configuration file.

Example for Traps:

```
createUser -e 0x01:02:03:04:05:A1:B2:C3:D4:E5 myUser MD5
myauthpassword DES myprivpassword
```

#### Where:

<code>-e &lt;engine:id&gt;</code>	specifies the Engine ID of the sending agent
<code>myUser</code>	security user name
<code>myauthpassword</code>	MD5 or SHA - authentication type and authentication password (optional parameter - do not use when authentication is not used)
<code>myprivpassword</code>	DES - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

## SNMPv3 Informs

Inform notifications require *two-way* communication. Inform messages expect a response. An **Inform** notification is essentially a Trap that gets acknowledged by the SNMP application that receives it. The sending SNMP application will repeat the Inform message until it gets an *I got it* response from the receiving SNMP application. In this case, the receiving SNMP agent is *authoritative*, which means the inform message should include the Security User credentials and the Engine ID of the receiving agent. However, because this is a two-way communication, it is possible for the sender to discover the Engine ID of the receiving agent. And because the Engine ID can be discovered, it is not necessary to specify an Engine ID in the SNMP Trap Service's configuration file. It is only necessary to provide security user/credential information in this file and let the sender discover the Engine ID as illustrated here.

Security information for Inform messages is defined using the `createUser` directive in the `snmptrapd.conf` file.

Example for Informs:

```
createUser myUser MD5 myauthpassword DES myprivpassword
```

---

**Where:**

---

*myUser* security user name

---

*myauthpassword* MD5 or SHA - authentication type and authentication password (optional parameter - do not use when authentication is not used)

---

*myprivpassword* DES - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

---

---

**NOTE:** Any time that the snmptrapd.conf file is changed, the SNMP Trap Service must be restarted. Refer to [Restarting the SNMP Trap Service](#) for more information.

---

# FlexViews

---

FlexViews are powerful tools that let you view a broad range of network configuration information presented in tables or other graphical formats including bar graphs, line graphs, and pie charts. Extreme Management Center Console ships with a comprehensive set of predefined FlexViews that you can select from to view the status and configuration information you need for your entire network. You can also use FlexViews to set values on devices when the FlexView contains MIB objects that are writable in devices.

FlexView data is searchable and sortable. In addition, you can easily modify and apply filters to the predefined FlexViews, and also create your own FlexViews to provide the kind of information you need to manage your network. FlexView data can be exported in delimited text and HTML formats. The information in FlexViews can be used to trigger events and can also be exported for remote monitoring as a Web page. You can use FlexViews to set device parameters by changing the value in columns that contain writable MIB objects. You can edit the parameters directly in the FlexView using the **Table Editor** row or you can use the **Guided Editor** to assist you with your changes.

In addition to viewing FlexViews in Console, you can also access [web-based FlexViews](#) that provide a convenient way for Operations people to view FlexView data without requiring access to Console. These views are accessible via a web browser and do not require the installation of any software (including Extreme Management Center) other than the browser itself.

When NetSight is initially installed, the Interface Summary right-panel tab is the default FlexView available in Console. From the Interface Summary FlexView you can open other FlexViews or create new FlexViews, if desired. For an introduction to using FlexViews, see [Working with FlexViews](#).



## How to Use FlexViews

---

FlexViews are a powerful network management tool. You can use FlexViews to set writable MIB objects, add instances (rows) to certain MIB tables on devices, and view a wide variety of information about the devices on your network as a table, bar graph, line graph, or pie graph. You access FlexViews from tabs in the right panel of the NetSight Console.

Instructions on:




- [Opening a FlexView](#)
  - [Printing a FlexView Table](#)
  - [Exporting FlexView Data](#)
- [Working With Graphs](#)
  - [Viewing Pie Graphs and Bar Graphs](#)
  - [Viewing Line Graphs](#)
  - [Exporting Graphs](#)
  - [Printing Graphs](#)
- [Editing Writable Values](#)
  - [Using the Guided Editor](#)
  - [Using the Table Editor](#)
- [Adding Instances to Certain MIB Tables](#)


### Opening a FlexView

When NetSight Console is initially installed, there is a default FlexView called Interface Summary, accessible from the **Interface Summary** tab in the right panel. A comprehensive set of FlexViews is available with NetSight Console. You can use the FlexView Properties window to customize these pre-defined views or create your own FlexViews to provide the exact kind of information you need to manage your network.

One or more FlexViews can be "**Floated**" into a separate window by clicking in a blank area of the FlexView toolbar and dragging the FlexView out of the Console main window. This allows viewing information from different FlexViews at the same time.

To open a FlexView:

1. Select one or more devices or device groups in the left panel. FlexViews always present information based on your selection in the left panel.
2. Click a FlexView tab in the right panel. If there are no FlexViews in the right panel, pull down the **Tools** menu and select **FlexView > Add FlexView Tab** to add a new FlexView tab. The new tab appears with the default title, *Interface Summary*.
3. Click your new FlexView tab.
4. Click the  button on the FlexView toolbar and select **Open** from the menu. A file browser window opens at the default FlexView path, where you can select one of the standard FlexViews.
5. Select a FlexView and click OK. The selected FlexView appears in the view and the name appears on the FlexView tab. When you open a FlexView, it is also added to the **FlexView** drop-down list.
6. Click the  (Retrieve button) to retrieve MIB values from the devices in the selected device group. The Retrieve button changes to a  (Stop button) and the progress of the polling is reported on the Console [Status](#) bar. When the polling is complete the button returns to a Retrieve button and the table is populated with the information retrieved from the devices.


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 other device-related views and a set of Table Tools that can be used to manage information in the table.

Use Console's table options and tools to filter, find, sort, print, and export information in the table, and to customize table settings. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

### *Printing a FlexView Table*

You can print all of the information or only selected rows from a FlexView table.

To print an entire FlexView table:

1. Select one or more devices/device groups in the left panel.
2. Open the FlexView that presents the information that you want to print and click Retrieve.
3. Click the  button on the FlexView toolbar and select **Print FlexView** from the menu. (You can also right-click on a header or anywhere in the table and select **Table Tools > Print** from the popup menu.)
4. Select a printer in the Print window and click **OK**.


To print selected rows from FlexView table:

1. Select one or more devices/device groups in the left panel.
2. Open the FlexView that presents the information that you want to print and click Retrieve.
3. Select the rows that you want to print.
4. Right-click on a header or on one of the selected rows in the table and select **Table Tools > Print Selection** from the popup menu.
5. Select a printer in the Print window and click **OK**.

### *Exporting FlexView Data*

You can export all of the information or only selected rows from a FlexView table.

To export an entire FlexView table:

1. Select one or more devices/device groups in the left panel.
2. Open a FlexView that presents the information that you want to export and click Retrieve.
3. Click the  button on the FlexView toolbar and select **Export FlexView** from the menu. (You can also right-click on a header or anywhere in the table and select **Table Tools > Export** from the popup menu.)
4. In the Save window, enter a filename, select a destination folder and file type (HTML or delimited text CSV spreadsheet-compatible format) and click **OK**.


To export selected rows from FlexView table:

1. Select one or more devices/device groups in the left panel.
2. Open the FlexView that presents the information that you want to export and click Retrieve.
3. Select the rows that you want to export.
4. Right-click on a header or on one of the rows selected in the table and select **Table Tools > Export Selection** from the popup menu.
5. In the Save window, enter a filename, select a destination folder and file type (HTML or delimited text CSV spreadsheet-compatible format) and click **OK**.

## Working with FlexView Graphs



FlexViews are capable of presenting information as a [Pie Graph](#), [Bar Graph](#), or [Line Graph](#) and printing or exporting information to a file or printer. The exported data is saved in CSV or HTML formats and graphs can be exported as BMP, JPG, PNG or TIFF formatted files.

### *Viewing Pie Graphs and Bar Graphs*

You can view the information presented in the FlexViews tables as a Pie Graph or Bar Graph. Pie Graphs and Bar Graphs let you view various combinations of information, graphically. Using the  (drop-down graph menu), you can export a graph as an image or print the graph. These features let you select one or more columns to assess network operation. Pie Graphs and Bar Graphs can be printed or exported as a BMP, JPG, PNG or TIFF formatted files.

The Bar Graph and Pie Graph are added above the Table and all of the Table features remain active while they are displayed.

To present information for the selected device group in a Pie Graph or Bar Graph:

1. Access a FlexView that presents the information that you want to show, either as a Pie Graph or Bar Graph.
2. Click the  (Pie Graph) or  (Bar Graph).
3. Click the **Columns** tab and select one or more columns from the list near the right side of the panel.
4. Click the **General Controls** tab and select the particular values that you want to capture in the Bar Graph or Pie Graph. The General Controls apply both when graphing values for a single column and when graphing

multiple columns.

---

**NOTE:** If you set **n=** to a number greater than the number of rows in the table, the graph will only show the rows available from the table; if you also check **Show Pie/Bar for other**, then a slice/bar for *other* will be shown as zero in the graph and the legend. For example, if you are graphing values for the highest five rows (or four rows with **Show Bar/Pie for other** checked), but have only four rows selected in the table, only four rows will be graphed and the slice/bar for *other* will be zero.

---

- With one column selected the values presented in a graph are a set quantity of the **Highest** or **Lowest** values. You can set the quantity to a value from 1 to 128. When **Show Bar/Pie for Other** is selected along with Highest or Lowest, the sum of the values for remaining rows are also shown as a separate element in the graph. For example, when Highest and Show Bar/Pie for Other are selected along with 10 in the quantity field, then the 10 highest values are represented by 10 bars or slices in the pie and another bar/slice is added to represent the sum of all other values for the selected column.



---

**NOTE:** When viewing a Bar Graph, if no bars appear after setting the quantity to a large sample, resize the width of the Console window to accommodate the number of sample.

---


- When multiple columns are selected, the selections change to **Min**, **Max**, and **Average**. Min shows the lowest value for each of the selected columns, Max shows the highest value for each of the selected columns and average shows the arithmetic mean value for each of the selected columns.

### Viewing Line Graphs

You can use Line Graphs to view the trends (over time) for various combinations of information. Using the  (drop-down graph menu), you can print and export a line graph as an image of the graph or export the raw data that was used to create the graph. Clicking  adds a Line graph above the table and adds a **Graph Data** tab to the table. All of the table features remain active while the Line Graph is running.

To present information for the selected device group in a Line Graph:

1. Set the Poll Frequency to any value ( in seconds) other than 0. Once you click Retrieve, Console will automatically start retrieving information from your left panel selection at the specified interval.

2. Click  (Line Graph). A blank Line graph is added above the table and a **Graph Data** tab is added to the table in the right panel. Also, the Line Graph Controls tab is now active in the tabbed panel at the right side of the window. The center panel is a legend showing the current columns selected.
3. Adjust the pane sizes to allow viewing the entire graph and access to tabbed panel settings.
4. Click the **Columns** tab and select one or more columns from the list.
5. Click the **General Controls** tab and select the particular values that you want to capture in the Line Graph. The General Controls apply both when graphing values for a single column and when graphing multiple columns.

**NOTE:** If you set **n=** to a number greater than the number of rows in the table, the graph will only show the rows available from the table; if you also check **Show line for other**, then a line for *other* will be shown as zero in the graph and the legend. For example, if you are graphing values for the highest five rows (or four rows with **Show Bar/Pie for other** checked), but have only four rows selected in the table, only four rows will be graphed and the line for *other* will be zero.


Also, when using a FlexView to create a line graph of zero-instanced rows, if **n=** is set to a number greater than or equal to the number of table rows and you also check **Show Line for other**, *other* appears in the legend and is graphed as zero in the graph, but *other* does not appear as a row in the Graph Data tab.

- With one column selected the values presented in a graph are a specific quantity of the **Highest** or **Lowest** values. You can specify the quantity as a value from 1 to 128. When **Show Line for Other** is selected along with Highest or Lowest, the sum of the values for remaining rows are shown as a separate line in the graph. For example, when Highest and Show Line for Other are selected along with 10 in the quantity field, then the 10 highest values are represented by 10 line in the graph and another line is added to represent the sum of all other values for the selected column. The selection of the highest or lowest rows to be plotted is determined by the values returned from the first query.

On this panel, you can enter an **X-Axis Label**, **Y-Axis Label**, and **Graph Label**. These fields allow entering text titles for the X and Y axes and the title that appears above the graph. These labels can only be defined when there is a single column selected. However, once the labels are entered, you can select additional columns and retain the

same labels.

- When multiple columns are selected, the selections change to **Min**, **Max**, and **Average**. Min shows the lowest value for each of the selected columns, Max shows the highest value for each of the selected columns, and Average shows the arithmetic mean value for each of the selected columns.
6. Click the **Line Graph Controls** tab and set:
- **Graph Type**
    - **Absolute Data** - plots the selected columns, as the accumulated value obtained during the selected poll interval, on a linear y-axes scale.
    - **Log Scale Absolute** - plots the selected columns, as the accumulated value obtained during the selected poll interval, on a logarithmic y-axes scale.
    - **Delta** - plots the selected columns, as the accumulated value that is amount of the change from the preceding value, per selected poll interval, on a linear y-axes scale.
    - **Rate** - plots the selected columns as a value per second, on a linear y-axes scale.
  - **Graph  $n$  Samples** to set the number of points to plot on the X-axis.
  - If you want to plot a moving average of values, check **Moving Avg - Samples** and set the number of samples that will be calculated to derive the moving average.
  - Check **Alarm Threshold** and enter a threshold value, if you will use the values being plotted to generate an alarm when the value computed for any selected column equals or exceeds the value specified in the field to the right of the checkbox. The computed value can be the Raw Data from the table or a Moving Average (using the number Samples specified for the Moving Average above). The alarm threshold can be triggered by **Raw Data** or a **Moving Avg** using **Absolute**, **Delta**, or **Rate** values for the data in the selected column(s). This feature will only generate alarms while the Line Graph is running.
7. If desired, check **Custom Y Axis** and enter values for the **Max Y Axis Value** and **Min Y Axis** fields to set the limits of the Y axis.


8. If desired, select an **Auto Export** option from the Auto Export the line graph data. This drop-down list lets you automatically export the graph data as either an HTML or .CSV file with each poll cycle.
9. Click **Retrieve**. The Retrieve button changes to  and the FlexView begins polling at the specified Poll Frequency and plotting the graph according to your selections.

A (blank) gap in a line indicates that there was no response from the device for that poll and no point was plotted. Dashed lines begin plotting the **Moving Averages** with the third poll cycle. The polling will continue until the Retrieve is clicked to stop polling.


### *Exporting Graphs*

All three graph types can be exported as an image file. The data used to produce line graphs (from the Graph Data tab) can also be exported as a data file. The graph image can be as a bitmap (.bmp), jpg (.jpg, .jpeg), PNG (.png), or tagged image format (.tiff) formatted file. Data files are either HTML (.htm, .html) or delimited text (.csv, .txt).

To export a graph image:

1. Click  (drop-down Graph Menu) and select **Export Graph**.
2. Navigate to the folder where you want to save the graph, enter a filename and select a file extension for the desired image format (.bmp, .jpg, .jpeg, .png, or .tiff).
3. Click **Save**.


To export graph data:

1. Click  (drop-down Graph Menu) and select **Export Data**.
2. Navigate to the folder where you want to save the graph data, enter a filename and select a file extension for the desired data format (.html or .txt, .csv).
3. Click **Save**.

### *Printing Graphs*

To print a graph:



1. Click  (drop-down Graph Menu) and select **Print Graph**.
2. Select a printer and set the print properties in the print dialog window.
3. Click **OK**.




## Editing Writable Values

You can change the value in FlexView table columns that contain a writable MIB object. You can edit the values directly in the FlexView table row using the **Table Editor** or you can use the **Guided Editor** to assist you with your changes. Only one table editing tool can be used at a time.

### *Using the Guided Editor*

The Guided Editor window functions like the Table Editor feature, but the window is divided into two sections: one containing instructions for editing the values and the other section contains the writable columns in the current FlexView where you can make changes.

To change values in a FlexView table using the Guided Editor:






1. Select one or more rows in a FlexView that contains columns with writable MIB objects, and click  to open the [Guided Editor](#) window.
2. Read the instructions in the top half of the view. (These are instructions that were added in the [FlexView Properties](#) window when the FlexView was created or edited.)
3. Check the writable objects that you are changing and enter the appropriate values as needed.
4. Click **Apply to Selected Rows** to enter your changes into the selected rows.
5. Click **Close** to dismiss the Guided Editor window.
6. To set the values that you've just changed in the affected devices, click  (Apply button). The values that you've changed in the table (marked with a ) are set in the selected devices. If the set is not successful, a red **X** appears in the rows where the set has failed.

### *Using the Table Editor*

The Table Editor appears as a single row at the bottom of a FlexView table. The writable fields in the table appear as an editable table cell or drop down list as appropriate for the object type (integer, boolean, text, etc.). Changing the value

in the Table Editor row alters the value for that entry in the row(s) selected in the table. Clicking Apply sets the current writable table values on the device(s).

To change values in a FlexView table using the Table Editor:

1. Access a FlexView that contains columns with writable MIB objects.
2. Click the  (Show/Hide Table Editor button) to show the Table Editor row at the bottom of the table.
3. Select one or more rows in the table. You can select multiple non-consecutive rows by holding the Control key while clicking or you can select consecutive rows by dragging the mouse pointer over the rows or by holding the Shift key and clicking the beginning and ending row in the range.
4. In the Table Editor row, change the value for your selected column(s). If you are selecting a value from a drop down list, the selection is immediately entered into the selected table cells. If you are typing a text string or integer value, typing **Enter** sets the value in the selected table cell(s). A green exclamation mark () appears in the cells where the value has been changed (but not Applied) and the **Apply** button becomes active.
5. To cancel your changes and restore the original values, click the  (Show/Hide Table Editor button) to hide the Table Editor before enforcing the table values.
6. To set the values that you've just changed in the affected devices, click  (Apply button). The values that you've changed in the table (marked with a ) are set in the selected devices. If the set is not successful, a red **X** appears in the rows where the set has failed.

---

**CAUTION:** Enforcing certain MIB objects can disable devices and cause interruptions to network operation. Do Not apply MIB values unless you are sure of the outcome.

---

## Adding Instances in MIB Tables

Use the Table Editor (the bottom row of the [Results table](#)) to add instances to certain tables in MIBs that support this feature. Tables that support this feature typically contain an object that shows the status of table rows.

For example, in the RMON MIB - **etherStatsTable**, the object *etherStatsStatus* indicates when the value in a particular row is valid, invalid, etc., which provides the means for adding a row in the etherStatsTable. Select *valid* to add a row, *invalid* to remove a row.

---

**NOTE:** Not all devices support *valid* directly. Some require a *create* set before a *valid* set.



---

You can add an instance to a table on a single device or to multiple devices, depending on your selection in the left panel. The particular FlexView where you are adding an instance must be configured:

- For a MIB table that supports adding instances
- Must not be set to Hide Instance
- Must not be set to Read Only

The instance added is always the lowest available (next) instance in the MIB table. So, if there are four instances in the table (1, 2, 5, 6), adding an instance will add instance 3. This is also true when adding instances to multiple devices; the next lowest available instance will be added to each device. In the following steps we'll use the 802.1Q Static VLAN FlexView to demonstrate adding and removing an instance.

To add an instance:




1. Open the 802.1Q Static VLAN FlexView (or another FlexView that supports the add instance feature).
  - a. Open the FlexView Properties window and remove the check marks from **Hide Instance** and **Read Only**.
  - b. **Save** the FlexView and **Close** the FlexView Properties window.
2. Select a device in the left panel and click  (Retrieve button).
3. Click  to enable the Table Editor.
4. Click an instance of the object. If the selected object is writable, the instance in the table editor row at the bottom of the table is active and you can enter an instance value or select **Next** from the drop-down list.

Using our example, we can select *Next* in the **Instance** column, edit the **VLAN Name** column to name this VLAN instance, then set the **VLAN Status** to *active*.

The new instance appears in the table with a green exclamation mark.

5. Click  (Apply button).
6. Click  (Retrieve button) to check the status of the new instance.

To remove an instance:

1. Click  to enable the Table Editor.
2. Click the instance being removed.
3. Locate the column containing the *status* object that allows adding or removing instances, and select the appropriate syntax from the drop-down list. In our example, the column is **VLAN Status** and the *destroy* syntax will remove the instance when the value is applied.
4. Click  (Apply).
5. Click  (Retrieve button) to check the status of the new instance.

---

**CAUTION:** Setting certain MIB objects can disable devices and cause interruptions to network operation. Do not set MIB values unless you are sure of the outcome.

---

## Related Information

For information on related windows:

- [FlexViews Tabs](#)
- [FlexView Properties Window](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Export the FlexView Catalog](#)

## How to Create and Modify FlexViews

---

FlexViews are a powerful network management tool. They can be configured to let you set certain MIB objects and show a wide variety of information about the devices on your network. You can create FlexViews using the FlexView Properties window and add FlexView tabs to the Console right panel to display the FlexView information as a table, bar graph, line graph, or pie chart. You can define as many FlexViews as needed to cover the information that you need to manage your network. And, for your ease of use, Console comes with a set of predefined FlexViews that lets you view a wide variety of information about the devices on your network.



When NetSight is initially installed, the Interface Summary right-panel tab is the default FlexView available in Console. From the Interface Summary tab you can open any of the FlexViews that come with Console or create new FlexViews, if desired. This Help topic provides instructions for creating a new FlexView. For information on opening an existing FlexView, see [Working with FlexViews](#).

Instructions on:

- [Creating a FlexView](#)
- [Modifying a FlexView](#)
- [Adding and Removing FlexView Tabs](#)

### Creating a FlexView

To create a new FlexView:

1. Click a FlexView tab in the right panel. If you have just installed NetSight, this would be the *Interface Summary* tab in the right panel. If there are no FlexViews tabs in the right panel, click the **Add FlexView Tab**  button in the Console toolbar. This will add an Interface Summary tab to the right panel.
2. Click the **FlexView**  button at the left end of the FlexView toolbar and select **New** from the drop-down menu. The **FlexView Properties** window opens.
3. There are two tabs in the FlexView Properties window: General and Columns. We'll begin by configuring the General tab.

4. The **General tab** is where you can edit FlexView parameters and add any notes to describe its purpose or special conditions. Configure the following parameters:
  - a. Select the **Instance type** for this FlexView. This setting affects the function and availability of the Port Tools options on the FlexView table right-click menu. The Instance type can be set to **802.1D Bridge Port**, **MIB-2 Interface**, or **Other**.
    - **802.1D Bridge Port** - Select 802.1D Bridge Port if the objects in the default request group for this FlexView are instanced by the MIB object `dot1dBasePort`. The Interface Statistics, RMON Ethernet Statistics, RMON History List, RMON Alarm/Event, RMON Packet Capture, I/F Enable, and I/F Disable options are added to the right-click menu.
    - **MIB-2 Interface** - Select MIB-2 Interface if the objects in the default request group for this FlexView are instanced by the MIB Object `IfIndex`. The Interface Statistics, RMON Ethernet Statistics, RMON History List, RMON Alarm/Event, RMON Packet Capture, I/F Enable, and I/F Disable options are added to the menu.
    - **Other** - no options are added to the right-click menu.
  - b. The **Export Type** setting lets you automatically export FlexView data with each table refresh. Files can be exported as HTML or CSV (spreadsheet compatible) file format. The exported information is saved by default in the `<user's home directory>\AppData\Roaming\NetSight\Console` directory, or you can specify a different export directory in the [FlexView Options](#) (Tools > Options). You can select one of six methods for the exported information:
    - **HTML** - Exports table information in HTML (Web format). This format lets you create an HTML file that can be used with a Web based status monitoring system. Refer to [How to Export FlexViews to a Web Monitor](#) for more information about using this feature. Only **Replace** or **Append** can be used with Web monitoring.
      - **Replace** - when exported, the file replaces the previously exported file. The filename is the FlexView name without a timestamp.

- **Append** - when exported, the current table information is appended to previously exported information in the export file. The filename is the FlexView name without a timestamp
- **Timestamp** - when exported, the current table information is saved in a separate file. The filename incorporates a timestamp (*year\_month\_day\_hour\_minutes\_seconds*) showing when the information was saved.
- **CSV** - Exports table information in spreadsheet format.
  - **Replace** - when exported, the file replaces the previously exported file. The filename is the FlexView name without a timestamp
  - **Append** - when exported, the current table information is appended to previously exported information in the export file. The filename is the FlexView name without a timestamp
  - **Timestamp** - when exported, the current table information is saved in a separate file. The filename incorporates a timestamp (*year\_month\_day\_hour\_minutes\_seconds*) showing when the information was saved.
- c. Select **MaxAccess/SuperUser** to use the Max Secure or SuperUser passwords for access to retrieve information and set values on devices.
- d. Select **Read Only** if you want to disable the table editor (via Table Editor or Guided Editor) for this table. Enforcing writable MIB objects will not be allowed when the table is set to Read Only.
- e. Select **Hide instance column** to hide the Instance column so that it will not be displayed in the FlexView.
- f. Select **Enable event notification** if objects in the FlexView will be used with the table Filter feature to create an alarm for a specific condition. For example, you can select a FlexView that contains columns of various errors and set a filter to show rows that contain greater than zero errors (Type 0 as the filter value, select a column of interest and set the Options for **Match as number** and **Not equal to**). The first time the table contains a row (with the first error), an alarm will be generated and recorded in the Console Event Log. An export file is also created to capture the content of the table when the alarm

occurred. The export file defaults to an HTML file and is saved to the <user's home directory>\AppData\Roaming\NetSight\Exports directory with the filename, <FlexView name>\_EventData\_<date>.html.

- g. Type a detailed description of this FlexView into the **Notes** field.
  - h. In the **FlexView Editing Instructions** field, provide detailed instructions for how this FlexView should be edited by the FlexView Guided Editor or Table Editor. The information that you provide here will appear at the top of the [Guided Editor window](#).
5. Click the **Columns Tab**. This tab lets you define the content and arrangement of the columns in your FlexViews. You can define columns that present the values for particular MIB objects or create expressions that combine specific MIB objects, to present information that shows the relationship between those objects. At the top left of the tab you can see two radio buttons that let you select a column type: SNMP and Expression. With **SNMP** selected, you can configure columns to show the values for specific MIB objects. With **Expression** selected, the Columns tab becomes an expression editor, providing functions that allow you to combine the values of specific MIB objects.
  6. Select SNMP to define the **SNMP Columns** for your new FlexView. The SNMP Columns view lets you select MIB objects for your FlexView columns, and arrange and name columns that will appear in your FlexView. The left panel contains three tabs. The Tree and List tabs let you select MIB objects. The Description tab shows the MIB description for a selected MIB object. Once an object is selected from the Tree or List tab, you can configure the object parameters in the right panel and then add the column to the Column Definition table (at the bottom of the window) by clicking the **New** button.

#### Tree tab

This tab shows the supported MIBs as a tree hierarchy. You can expand the tree to select MIB objects or use the Find Feature to locate the object that you want to appear in your FlexView.

#### List tab

This tab presents MIB objects in a table. A right-click menu provides find and filter features to help you locate specific MIB objects in the list. You access these Table Tools through a right-mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.



### Description

This tab shows the text description that appears in the MIB for the selected object.

### Find

The **Find Feature** lets you search the tree to locate a specific MIB Object by typing all or part of a text string for a particular Object ID or Description into the **Find what** field, selecting a search option, and clicking **Find**. For more information on how to select options refer to Help on the Find toolbar.

To use the SNMP Columns view to define the columns that will appear in this FlexView:

- a. Select a MIB object from the left panel Tree or List tab.
- b. Type a column name for this MIB object into the **Column Name** field.
- c. Select a **Request Group** from the drop-down list. NetSight Console supports multiple SNMP requests. You can assign a particular MIB object to one of four request groups corresponding to a particular grouping of SNMP requests sent to devices. By grouping MIB objects, you can separate requests for objects that may not be supported on a particular device from objects that are. Request Groups are staged and queried in the following order: default, group 2, then group 3 and group 4. For more information, see the [Request Groups](#) and the [Indirect Instancing](#) Help topics.
- d. The **Instance Column** setting allows using the data returned in the column selected in the drop-down list as the instance for the MIB object selected for this column. The referenced column must be mapped to the **Default** request group or to a request group that has a lower number than the group for the referencing column. For more information, see the [Request Groups](#) and the [Indirect Instancing](#) Help topics.
- e. Check **Extract Instance** if you are using Console's Extract Instance feature and set the **Offset** value to define the starting position within the instance string and the **Length** to specify the number of elements to extract. This feature allows users having an in-depth knowledge of MIBs to extract data from one instance value and use that data as the instance for retrieving the value of another MIB object. For more information see the [Extract Instance](#) Help topic.

- f. If you've selected a writable object for this column, you can click the **Configure Instructions** for the table editor button. It opens the **Column Instructions** window where you can add text to describe how or why a user may wish to set a particular value for this column. Enter your instructions into the text area and click **OK** to create instructions for this column.
- g. Type a description for this column into the **Notes** panel.
- h. Click **New**. The column appears in the **Column Definitions Table** at the bottom of the properties window. You can add up to 61 columns (for a total of 64 columns) to a FlexView.
- i. Repeat steps **a** through **h** until you've selected/defined all of the SNMP columns for this FlexView.

---

**NOTE:** You can change the definition for a column that you've added by selecting the column from the Column Definitions Table, changing the definition, and then clicking **Apply**.

---

7. If you are adding expression columns to your FlexView, select the **Expression** radio button at the top of the tab. Otherwise, go on to [Step 8](#). The Expression Editor is a powerful tool that lets you enhance the value and clarity of FlexView tables by adding columns that contain data manipulating routines. These routines can access data in other columns in the table, and combine them with data from stored variables, constants, system functions, and user-defined functions to come up with new values to be displayed in the column. A conceptual discussion of the language of the Expression Editor is provided in the [FlexView Concepts - Expression Editor](#) topic.

---

**NOTE:** The following is only an outline of the order of steps used to create a column routine or table function. This is because the Expression Editor is an advanced feature of FlexViews that uses a programming language similar to the **C** programming language and the possible combinations of expressions are too numerous to describe within this topic. They are only limited by your imagination and skill with the language of expressions. You should be familiar with this language before attempting to create a column routine. Refer to [FlexView Concepts - Expression Editor](#) for a more detailed description of the FlexView Expression Editor features and the language of expressions. Refer to the [FlexView Properties Window](#) Help topic for information on specific fields in the window.

---

To add Expression columns:

- a. Select the **Column Routine** tab in the Column Routine/Function panel and type a name for your new column.
- b. Type expressions directly into the expression work area of the Expression tab or use the [Expression Wizard](#) to define the expressions for this column routine.
- c. When you have completed the routine, click **New** to add the column. New automatically checks the syntax of your expressions. The Status field reports **Passed** if there are no syntactic errors in the column routine. The syntax check does not check the logic of your expressions, only the syntax. When errors are found, the Status field identifies the error and, when possible, suggests corrective steps. Your new column is added to the Column Definitions Table at the bottom of the view.

**NOTE:** You can change the definition for a column that you've added by selecting the column from the Column Definitions Table, changing the definition, and then clicking **Apply**.

To add a table function:

- a. Select the **Function** tab in the Column Routine/Function panel and type a name for your new function.
- b. Type expressions directly into the expression work area of the Expression tab or use the [Expression Wizard](#) to define the expressions for this function.
- c. When you have completed the function, click **New**. New automatically checks the syntax of your expressions. The Status field reports **Passed** if there are no syntactic errors in the function. The syntax check does not check the logic of your expressions, only the syntax. When errors are found, the Status field identifies the error and, when possible, suggests corrective steps. Your new function is added to the Table Functions folder. You can access your new function by selecting **Function>Table** from the Expression Wizard, and use it in expressions within the table where it was created.

**NOTE:** You can change the definition for a function that you've added by selecting the function from the Functions tab, changing the definition, and then clicking **Apply**.

8. You can rearrange the order of the columns if necessary. Select a column in the Column Definitions Table and drag it to the right or left to adjust the order of your columns. The Column Definitions Table shows the order of the columns that will appear in the FlexView table. **Delete** removes the currently selected column from the Column Definitions Table.

9. When you are satisfied with your changes, click **OK**. The FlexView file browser opens where you can name and save this FlexView. By default, FlexViews that you've created are saved to `<user's home directory>\AppData\Roaming\NetSight\Console\My FlexViews` directory. To save to another location, navigate to a directory where you want to save your FlexView and type a name for this FlexView into the File name field. This is the name that will appear on your FlexView tab, so try to make the name short, but meaningful.

## Modifying a FlexView



You can add columns, rearrange the order of columns, and rename an existing FlexView using the FlexView Properties window. The following steps describe accessing the FlexView Properties window, but do not cover details of adding columns since that is accomplished in the same way as described in the section for [Creating a FlexView](#).

---

**NOT E:** Any pre-defined FlexViews that you modify and save will be overwritten when you update to a new release (or re-install the same release) of Console. However, your modified FlexViews will be retained and can be retrieved from the `<install directory>\NetSight\.installer\backup\current\appdata\System\FlexViews` folder following installation.

---

To modify an existing FlexView:

1. Select the FlexView that you want to modify from the **FlexView** drop-down list or click the  button on the FlexView toolbar and select **Open** from the menu to open a specific FlexView that is not on the list.
2. Click the  button on the FlexView toolbar and select **Properties** from the menu. The FlexView Properties window opens.
3. Click the **General** tab. Refer to [Step 4 in the Creating a FlexView](#) section for information about configuring General parameters.
4. Click the **Columns** tab. If you are adding columns or changing column definitions, refer to [Step 6 in the Creating a FlexView](#) section for information about adding columns. When you've finished adding columns, return here to rearrange columns for this FlexView.
5. You can remove unwanted columns and rearrange the order of the columns here if necessary.

- a. Select a column in Column Definitions Table at the bottom of the view and drag it to the left or right to reposition the column.
- b. Click **Delete** to remove the currently selected column from the Column Definitions Table.

---

**NOTE:** Clicking **Reload** before you have saved any changes to the FlexView lets you restore the settings to the previously saved version.

---

6. When you are satisfied with your changes, click **OK** or if you are going to save this FlexView under a different name, click **Save As** and rename the file. FlexViews that you've created are saved to `<user's home directory>\AppData\Roaming\NetSight\Console\My FlexViews` directory. To save the FlexView to another directory, navigate to a directory where you want to save your FlexView and type a name for this FlexView into the File Name field. This is the name that will appear on your FlexView tab, so try to make the name short, but meaningful.
7. Click **Close** to exit from the FlexView Properties.



## Adding and Removing FlexView Tabs

When Console is first installed, a *default* FlexView tab (Interface Summary) is available in the right panel. Use these instructions to add or remove other FlexView tabs from Console.

### *Adding Tabs*


You can add up to ten FlexView tabs. Tabs that you create are available when Console is restarted.

To add a new FlexView tab:

1. Click  (**Add FlexView Tab**) on the toolbar. (You can also pull down the **Tools** menu and select **FlexView > Add FlexView Tab** or type Control-t.) The new tab appears with the default title, *Interface Summary*. Once the tab is added you can select a specific FlexView and its title will appear on the tab.
2. Click the new tab and select a FlexView from the **FlexView** drop-down list or click the  button on the FlexView toolbar and select **Open** from the menu to open a specific FlexView. The name of the selected FlexView now appears on the tab.

## *Removing Tabs*

To remove a new FlexView tab:

1. Select the tab that you want to remove.
  2. Click  (**Remove FlexView Tab**) on the toolbar. (You can also pull down the **Tools** menu and select **FlexView > Remove FlexView Tab** or type Control-r.) The tab is removed without further confirmation.
- 

## **Related Information**

For information on related windows:

- [FlexView Concepts](#)
- [FlexView Tabs](#)
- [FlexView Properties Window](#)

For information on related tasks:

- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## FlexView Tabs

---

FlexViews are powerful tools that you can use to display a broad range of network configuration information presented in tables or other graphical formats including bar graphs, line graphs, and pie charts. When NetSight is initially installed, the Interface Summary right-panel tab is the default FlexView available in Console. It is one of a comprehensive set of FlexViews available with Console. From the Interface Summary FlexView you can open other FlexViews or create new FlexViews, if desired. For an introduction to using FlexViews, see [Working with FlexViews](#).

---

**TIP:** One or more FlexViews can be "**Floated**" into a separate window by clicking in a blank area of the FlexView toolbar and dragging the FlexView out of the Console main window. This allows viewing information from different FlexViews at the same time.

---

This Help topic provides information about the FlexView table and toolbars. For information on displaying FlexViews in the other available graphical formats, see the following topics:

- [FlexViews - Pie Graphs](#)
- [FlexViews - Line Graphs](#)
- [FlexViews - Bar Graphs](#)

## Sample FlexView

The screenshot shows the 'Physical Entity Listing' window in a network management application. The window has a toolbar with a dropdown menu and a 'Poll Frequency' set to 0. The main area displays a table with the following columns: IP Address, Instance, Name, Class, Description, Vendor Type, Parent Rel Pos, and Hdr. The table lists various hardware components like chassis, slots, backplane, power supplies, fans, modules, and ports, all associated with the IP address 10.20.20.138.

IP Address	Instance	Name	Class	Description	Vendor Type	Parent Rel Pos	Hdr
10.20.20.138	1	chassis-1	chassis	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhy7C103	-1	
10.20.20.138	11	slot-1	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3Module...	1	
10.20.20.138	12	slot-2	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3Module...	2	
10.20.20.138	13	slot-3	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3Module...	3	
10.20.20.138	32	backplane-1	backplane	Enterasys Networks, Inc. Matrix N3; 3 SI...	0.0	1	
10.20.20.138	41	powersuppl...	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3PowerS...	1	
10.20.20.138	42	powersuppl...	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3PowerS...	2	
10.20.20.138	46	powersuppl...	powerSupply	Enterasys Networks, Inc. Matrix N3; AC ...	etsysOidPhy7C203x1	1	
10.20.20.138	51	fan-slot-1	container	Enterasys Networks, Inc. Matrix N3; 3 SI...	etsysOidPhyN3FanTra...	1	
10.20.20.138	56	fan-1	fan	Enterasys Networks, Inc. Matrix N3; Fan...	etsysOidPhy7C403	1	
10.20.20.138	72	module-2	module	Enterasys Networks, Inc. DFE-Platinum ...	etsysOidPhy7H4202x72	1	0
10.20.20.138	73	module-3	module	Enterasys Networks, Inc. DFE-Platinum ...	etsysOidPhy7G4280x19	1	2
10.20.20.138	21001	fe.2.1	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	1	1
10.20.20.138	21002	fe.2.2	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	2	1
10.20.20.138	21003	fe.2.3	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	3	1
10.20.20.138	21004	fe.2.4	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	4	1
10.20.20.138	21005	fe.2.5	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	5	1
10.20.20.138	21006	fe.2.6	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	6	1
10.20.20.138	21007	fe.2.7	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	7	1
10.20.20.138	21008	fe.2.8	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	8	1
10.20.20.138	21009	fe.2.9	port	Enterasys Networks, Inc. 100BASE-TX ...	etsysOidPhyFrtPnlFast...	9	1

## FlexView Toolbar



### FlexView Button

Click this button to access a drop-down menu with the following options:

- **New** - opens the [FlexView Properties](#) window where you can define a new FlexView.
- **Open** - opens the FlexView file browser where you can select a FlexView for viewing (and add it to the FlexView drop-down list) or export a FlexView catalog.
- **Reload** - loads the currently selected FlexView, clearing all table information and graph settings to their defaults for the selected FlexView.
- **Save** - saves the current FlexView.
- **Find in FlexView** - Opens the Find toolbar at the top of the currently selected FlexView.
- **Filter FlexView** - Opens the Filter toolbar at the top of the currently selected FlexView.
- **Sort FlexView** - Opens the Sort toolbar at the top of the currently selected FlexView.



- **Export FlexView** - Exports the currently selected FlexView. When a Pie Chart or Bar Graph is displayed, the information is exported to a GIF formatted image file. When a table is displayed, the table information is exported to an HTML file or Delimited Text file.
- **Print FlexView** - Prints the currently selected FlexView.
- **Save As** - opens a file browser where you can select a location and name for the current FlexView before saving.
- **FlexView Data Source** - opens the FlexView Data Source window showing a list of devices that are the source of information shown in the FlexView.
- **Properties** - opens the [FlexView Properties](#) window where you can rearrange columns, change the polling settings, enable event notification, export FlexView information for Web monitoring, lock the FlexView as *Read only*, and hide the instance column. This view also lets you edit the elements being presented in the view.

### FlexView

This drop-down list lets you select one of the currently opened FlexViews for viewing.



### View Type Buttons

You can display the information retrieved from devices in a table, as a pie chart, bar graph, or line graph by clicking the associated icon.

### Poll Frequency

This drop-down list lets you select the interval between polling the selected device(s) for information. You can select 0 for no polling, a preset poll interval of 10, 20, or 30 seconds, or you can enter a value from 1 second up. If you select 0 and click the Retrieve button, this forces a single poll cycle to retrieve information from the selected device.



### Guided Editor


This button opens a [Guided Editor](#) window. You can use the Guided Editor to change the value in FlexView table columns that contain writable MIB objects. The Guided Editor window performs the same function as the Table Editor feature, but provides instructions and information for editing the values. The Guided Editor feature cannot be used at the same time as the Table Editor.

 **Show/Hide Table Editor**

This button is active only when writable MIB objects appear in the current FlexView. This button toggles the Table Editor (see below) that allows you to change the value of writable objects in the table.

**Table Editor**

The Table Editor row is visible when the Show/Hide Table Editor button is toggled to make the Table Editor visible. Columns that contain a writable MIB object will appear in the Table Editor as an editable field or drop-down list as appropriate for the object type (integer, boolean, text, etc.).

Changing the value in the Table Editor row alters the value for that entry in the row(s) selected in the table. As values are 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 will cancel your changes, restore the original values, and hide the Table Editor. Clicking **Apply** sets the values that you've changed in the selected devices, removes the !, and hides the Table Editor row. If the set is not successful, a red X appears in the rows where the set has failed. The Table Editor feature cannot be used at the same time as the Guided Editor.

 **Apply**

This button is active when the Table Editor (see above) is enabled. Using the Table Editor, you can edit the value of specific writable MIB objects and then click **Apply** to set the current writable table values on the devices in the currently selected device group. **Apply** sets the value in the selected devices, clears the ! from the table, and hides the table editor row. If the set is unsuccessful, a red X marks the rows where the set failed.

---

**CAUTION:** Applying certain MIB objects can disable devices and cause interruptions to network operation. Do not apply MIB values unless you are sure of the outcome.

---

 **Retrieve**

This button controls polling the devices in the selected device group. Initially, polling is stopped and a green Retrieve button is displayed. Polling is started by clicking the Retrieve button and the icon changes to either a red Stop symbol if only a single poll is taking place or a yellow Auto Retrieving symbol while polling is in progress at the defined Poll Frequency. You can stop the poll by clicking either the red or yellow symbol.

## FlexView Table


All FlexView tables are created with IP Address and Instance (system-defined) columns. They cannot be removed from the FlexView. However, the instance can be hidden by checking **Hide Instance Column** in the [FlexView Properties](#) window. IP Address cannot be hidden.

---

**NOTE:** The Current Link column of the Interface Summary FlexView will show a *dormant* status for links that are attached to an active Link Aggregation Group (LAG).

---

## 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 the Table Tools popup menu that provides access to other device-related views and a set of table tools that can be used to manage information in the table.

## Console Main Toolbar Buttons

These FlexView buttons are available from the NetSight Console main toolbar.



### Add FlexView Tab

Adds a new FlexView tab in the right panel. The new tab appears with the default title, *Interface Summary*. Once the tab is added you can select a specific FlexView and its title will appear on the tab. This button provides an alternative access to the Console Tools menu **FlexView > Add FlexView Tab** option (typing Control-t also adds a tab).



### Remove FlexView Tab

Deletes the currently selected FlexView tab from the right panel. This button provides an alternative access to the Console Tools menu **FlexView > Remove FlexView Tab** option (typing Control-r also removes the currently selected tab).


---

## Related Information

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

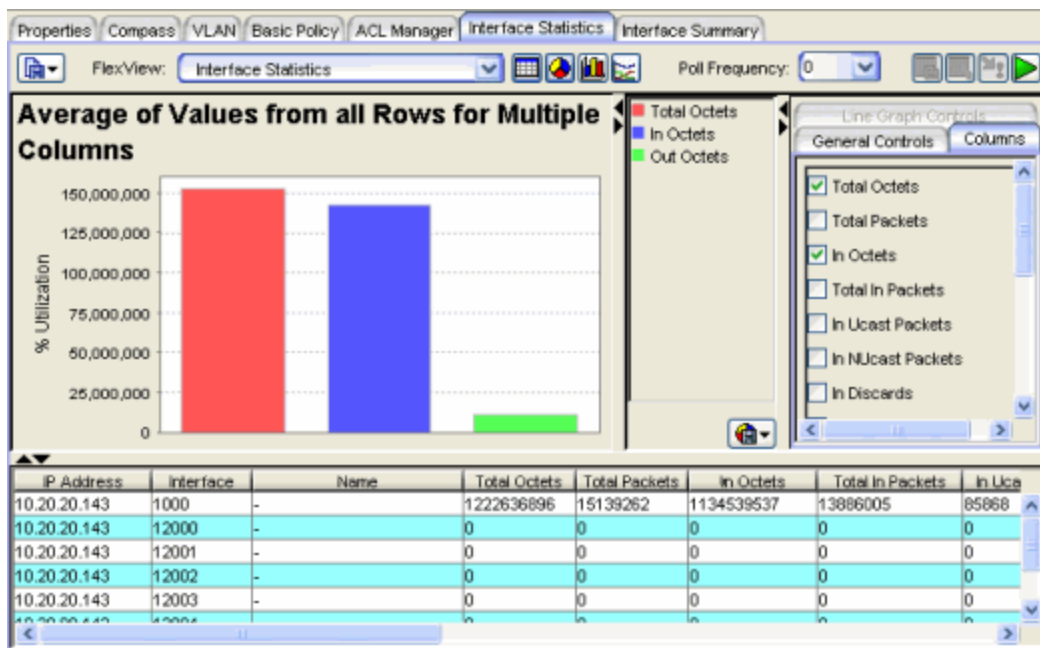
## FlexView Bar Graphs

In a FlexView tab, click the Bar Graph button  in the FlexView toolbar to display the FlexView data in a bar graph format. The bar graph is situated above the FlexView table; all of the table features remain active while the bar graph is displayed. The bar graph area is split into three sections:

- **Graph** - the left section shows the actual bar graph
- **Legend** - the middle section displays a legend that relates the colors in the graph to the attributes being displayed in the graph
- **Graph Settings** - the right section contains two tabs that allow you to configure the bar graph

A bar graph provides a snapshot showing information as vertical bars. Each color-coded bar can represent either independent or related attribute values. Bar graphs are the best tool for comparing unrelated columns. For example, to present a profile of received vs. transmitted packets for a specific number of samples or to show a correlation between two FlexView columns. Holding the mouse pointer over a particular bar will show a *tool tip* that identifies that value.

### Sample Bar Graph.





### Drop-Down Menu Button

Click this button to display bar graph menu options:

- **Export Graph** - This option lets you export the currently displayed bar graph information as a BMP, JPG, PNG, or TIFF formatted image file.
- **Print Graph** - This option lets you print the currently displayed bar graph.

## Bar Graph Settings

The Columns tab and General Controls tabs are used to configure the bar graph. In the Columns tab, select the columns you want displayed in the bar graph. The General Controls tab changes depending on the number of columns selected in the Columns tab.

### With multiple columns selected

With multiple columns selected, the choices on the General Controls tab let you choose the **Maximum**, **Average**, or **Minimum** values from all rows. You can compare columns to show the highest, average or lowest values for each of the selected columns.

**NOTE:** Some FlexViews are intended to plot only Single column values. For example, the (Interface) **Port Utilization - Graph** FlexView that is provided with Console shows port utilization by plotting the single column, *Total Octets* for the five highest interfaces. If multiple columns are selected for this FlexView, the graph, as designed, can no longer plot port utilization. Instead, it will show the averages for the selected columns across all interfaces.

### With a single column selected

With only one column selected in the Columns tab, the General Controls tab lets you specify the following information.

General Controls - Single Column Selected

The screenshot shows a dialog box titled "Line Graph Controls" with two tabs: "General Controls" (selected) and "Columns". Under "Use Data From:", there are two radio buttons: "Highest n Rows" (selected) and "Lowest n Rows". Below this is a text input field for "n =" containing the number "5". There is a checked checkbox for "Show Bar for 'other'". At the bottom, there are three text input fields: "X Axis Label" (empty), "Y Axis Label" (containing "% Utilization"), and "Graph Label" (empty).

**Highest n Rows, Lowest n Rows, n=**

With a single column selected, you can show the data for the specified ( $n$ ) rows with the highest or lowest values for the selected column.

**NOTE:** If you set **n=** to a number greater than the number of rows in the table, the graph will only show the rows available from the table; if you also check **Show Bar for other**, then a bar for *other* will be shown as zero in the graph and the legend. For example, if you are graphing values for the highest five rows (or four rows with **Show Bar for other** checked), but have only four rows selected in the table, only four rows will be graphed and the bar for *other* will be zero.

**Show Bar for Other**

When checked, a bar labeled *Other* is added to the graph to show the sum of the values from all of the rows not specifically selected on the Columns tab.

**X-Axis Label, Y-Axis Label, Graph Label**

These fields allow entering text titles for the X and Y axes and the title that appears above the graph.

---

**NOTE:** These labels can only be defined when there is a single column selected. However, once the labels are entered, you can select additional columns and retain the same labels.

---

## Related Information

For information on related windows:

- [FlexView Properties Window](#)
- [FlexView Pie Graphs](#)
- [FlexView Line Graphs](#)


For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)



## FlexView Line Graphs


---

In a FlexView tab, click the Line Graph button  in the FlexView toolbar to display the FlexView data in a line graph format. You can use line graphs to view the trends (over time) for various combinations of information. The line graph is situated above the FlexView table; all of the table features remain active while the line graph is displayed. The line graph area is split into three sections:

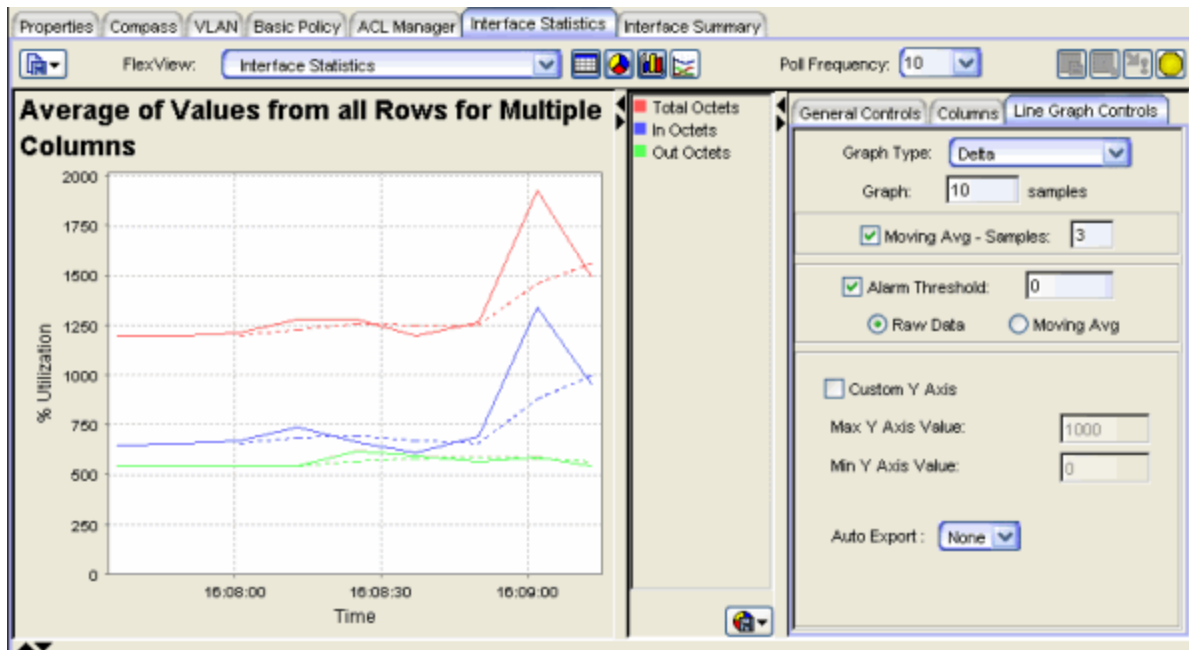
- **Graph** - the left section shows the actual line graph
- **Legend** - the middle section displays a legend that shows the particular column or row associated with the colors for each line
- **Graph Settings** - the right section contains three tabs that allow you to configure the line graph

When you display a line graph it also adds a **Graph Data** tab to the table below. The **Graph Data** tab shows the graph data in tabular format. Each poll cycle appends rows to the table to show the values returned for the selected data. The **Sample** column is incremented with each poll cycle. The Graph Data table is limited to 65,000 rows and wraps around, overwriting rows 1, 2, etc. after reaching this limit.

Scientific notation is used in the Graph Data to show very large and very small values. Scientific notation presents values in the base 10, using an exponent and decimal point to present these values. For values less than one, the exponent is expressed as a negative number to show a number of decimal places to move to the left the decimal point to express the same value as an integer. For example, the value 0.0000345 could be expressed in scientific notation as 345e-7 or 3.45e-5. For values greater than one, the exponent is expressed as a positive number to show a number of decimal places to move to the right the decimal point to express the same value as an integer.. For example, 3,450,000 could be expressed as 3.45e6 or 345e4.

The **Poll Frequency** setting determines the interval for the X axis (time division) shown on the graph. You can select a pre-defined poll setting from the drop-down list or type a value directly into the Poll Frequency field. The frequency must be set to a non-zero value and the  (Retrieve button) must be clicked to plot information trends with the line graph. When there is no information returned from a device for a poll, the line is interrupted (blank) for that poll interval. Holding the mouse pointer over a particular line will show a *tool tip* that identifies that value.

### Sample Line Graph



#### Drop-Down Menu Button

Click this button to display line graph menu options:

- **Export Graph** - This option lets you export the currently displayed line graph information as a BMP, JPG, PNG, or TIFF formatted image file.
- **Print Graph** - This option lets you print the currently displayed line graph.
- **Export Data** - Opens a file browser where you can select a name and location for exporting the information currently displayed in the Graph Data tab of the table to a file. The file is exported as an HTML or spreadsheet-compatible CSV file. The default format is HTML and the default filename is `<current FlexView name>_Graph_Data.html`. For example, `Interface_Summary_Graph_Data`. There is no default name when exported as CSV.

## Line Graph Settings

The General Controls tab, the Columns tab, and the Line Graph Controls tab are used to configure the line graph. In the Columns tab, select the columns you want displayed in the line graph.

## General Controls Tab

The settings on this tab change according to the number of columns selected in

the Columns tab.

### With multiple columns selected:

With multiple columns selected in the Columns tab, the General Controls tab lets you choose the **Maximum**, **Average**, or **Minimum** values from all rows. You can compare columns to show the highest, average, or lowest values for each of the selected columns.

**NOTE:** Some FlexViews are intended to plot only single column values. For example, the (Interface) **Port Utilization - Graph** FlexView that is provided with Console shows port utilization by plotting the single column, *Total Octets* for the five highest interfaces. If multiple columns are selected for this FlexView, the graph, as designed, can no longer plot port utilization. Instead, it will show the averages for the selected columns across all interfaces.

### With a single column selected:

With only one column selected in the Columns tab, the General Controls tab lets you specify the following information.

#### General Controls Tab - Single Column Selected

The screenshot shows the 'General Controls' tab with the following settings:

- Use Data From:**
  - Highest n Rows
  - Lowest n Rows
- n =** 5
- Show Line for 'other'
- X Axis Label:** (empty text box)
- Y Axis Label:** % Utilization
- Graph Label:** (empty text box)

### Highest n Rows, Lowest n Rows, n=

With a single column selected, the graph shows the data for the specified  $n$  rows with the highest or lowest values for the selected column. A (blank) gap in a line indicates that there was no response from the device for that poll and no point was plotted. The selection of the highest or lowest rows to be plotted is determined by the values returned from the first query and

these rows will remain selected regardless of the values returned from subsequent queries.

---

- NOTES:**
1. If you set **n=** to a number greater than the number of rows in the table, the graph will only show the rows available from the table; if you also check **Show Line for other**, then a line for other will be shown as zero in the graph and the legend. For example, if you are graphing values for the highest five rows (or four rows with **Show Line for other** checked), but have only four rows selected in the table, only four rows will be graphed and the line for other will be zero.
  2. When using a FlexView to create a line graph of zero-instanced rows, if **n=** is set to a number greater than or equal to the number of table rows and you also check **Show Line for other**, *other* appears in the legend and is graphed as zero in the graph, but *other* does not appear as a row in the Graph Data tab.
- 

### Show Line for other

When checked, a line labeled *Other* is added to the graph to show the sum of the values from all of the rows not specifically selected on the Columns tab.

### X-Axis Label, Y-Axis Label, Graph Label

These fields allow entering text titles for the X and Y axes and the title that appears above the graph.

---

**NOTE:** These labels can only be defined when there is a single column selected. However, once the labels are entered, you can select additional columns and retain the same labels.

---

## Line Graph Controls Tab

This tab determines how the selected columns will be presented in the graph.

### Sample Line Graph Controls

#### Graph Type

This drop-down list lets you select from four graph types:

- Absolute - plots the selected columns as the accumulated value obtained during the selected poll interval, on a linear y-axis scale.
- Log Absolute - plots the selected columns as the accumulated value obtained during the selected poll interval, on a logarithmic y-axis scale.
- Delta - plots the selected columns as the accumulated value that is amount of the change from the preceding value, per selected poll interval, on a linear y-axis scale.
- Rate - plots the selected columns as a value per second, on a linear y-axis scale.

#### Graph: $n$ samples

This setting determines the number of points to plot on the X-axis.

#### Moving Avg - Samples

When checked, the value that is plotted on the graph will be calculated as the arithmetic mean derived from the number of preceding samples specified in the associated **Samples** field.

### Alarm Threshold

When checked, an alarm is generated when the value computed for any selected column equals or exceeds the value specified in the field to the right of the checkbox. The computed value can be the Raw Data from the table or a Moving Average (using the number Samples specified for the Moving Average above). The alarm threshold can be triggered by **Raw Data** or a **Moving Avg** using **Absolute**, **Delta**, or **Rate** values for the data in the selected column(s). This feature will only generate alarms while the Line Graph is being displayed.

### Custom Y Axis

When checked, the Max Y Axis Value and Min Y Axis Value fields are enabled to allow you to set the limits of the Y axis by setting a minimum and/or maximum value.

### Auto Export

This drop-down list lets you export the graph data as either an HTML or CSV file.

---

## Related Information

For information on related windows:


- [FlexView Properties Window](#)
- [FlexView Pie Graphs](#)
- [FlexView Bar Graphs](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## FlexView Pie Graphs

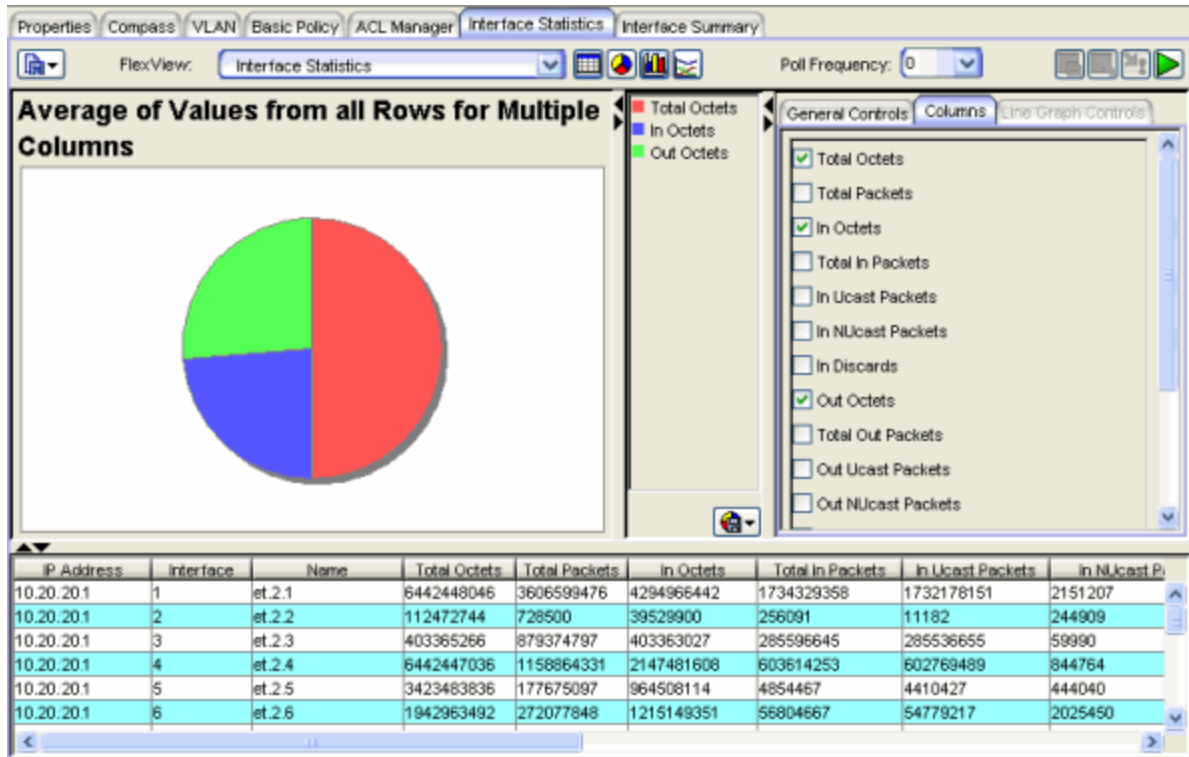
---

In a FlexView tab, click the Pie Graph button  in the FlexView toolbar to display the FlexView data in a pie graph format. The pie graph is situated above the FlexView table; all of the table features remain active while the pie graph is displayed. The pie graph area is split into three sections:

- **Graph** - the left section shows the actual pie graph
- **Legend** - the middle section displays a legend that shows the particular column or row associated with the colors in the pie
- **Graph Settings** - the right section contains two tabs that allow you to configure the pie graph

A pie graph provides a snapshot showing information as slices in a pie. Each color-coded slice represents a particular column or row as a percentage of the pie. Pie graphs are best used for understanding the relationship between related values (columns). For example, to determine what percentage of received packets were unicast vs. non-unicast, you could select the *In Unicast Packets* and *In Non-Unicast Packets* columns and easily see the contribution from each to the all received packets. Holding the mouse pointer over a particular slice will show a *tool tip* that identifies that value.

### Sample Pie Graph



#### Drop-Down Menu Button

Click this button to display pie graph menu options:

- **Export Graph** - This option lets you export the currently displayed pie graph information as a BMP, JPG, PNG, or TIFF formatted image file.
- **Print Graph** - This option lets you print the currently displayed pie graph.

## Pie Graph Settings

The Columns tab and the General Controls tabs are used to configure the pie graph. In the Columns tab, select the columns you want displayed in the pie graph. Each column that is selected will be displayed as a slice in the pie. If only one column is selected, the pie shows the share of the pie for the specific number of rows set in the General Controls tab as a slice in the pie. The General Controls tab changes depending on the number of columns selected in the Columns tab.

With multiple columns selected:



With multiple columns selected, the choices on the General Controls tab let you choose the **Maximum**, **Average**, or **Minimum** values from all rows. You can compare columns to show the highest, average or lowest values for each of the selected columns.

---

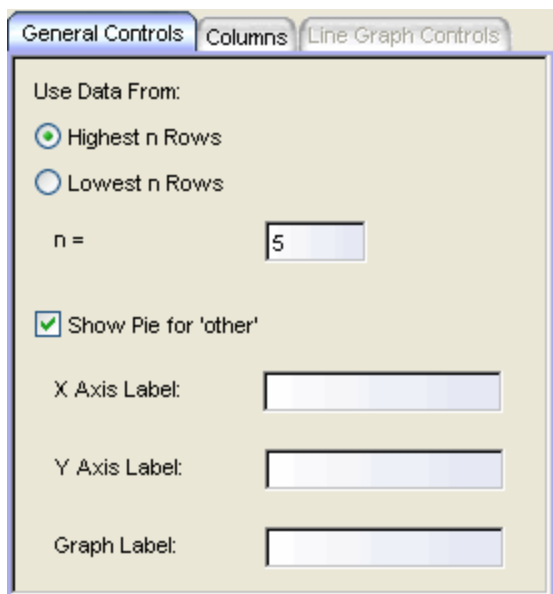
**NOTE:** Some FlexViews are intended to plot only Single column values. For example, the (Interface) **Port Utilization - Graph** FlexView that is provided with Console shows port utilization by plotting the single column, *Total Octets* for the five highest interfaces. If multiple columns are selected for this FlexView, the graph, as designed, can no longer plot port utilization. Instead, it will show the averages for the selected columns across all interfaces.

---

With a single column selected:

With only one column selected in the Columns tab, the General Controls tab lets you specify the following information.

*General Controls - Single Column Selected*



The screenshot shows a dialog box with three tabs: "General Controls" (selected), "Columns", and "Line Graph Controls". Under "Use Data From:", there are two radio buttons: "Highest n Rows" (selected) and "Lowest n Rows". Below these is a text input field labeled "n =" containing the number "5". There is a checked checkbox labeled "Show Pie for 'other'". At the bottom, there are three text input fields labeled "X Axis Label:", "Y Axis Label:", and "Graph Label:", all of which are currently empty.

**Highest n Rows, Lowest n Rows, n=**

With a single column selected, you can show the data for the specified ( $n$ ) rows with the highest or lowest values for the selected column.

**NOTE:** If you set **n=** to a number greater than the number of rows in the table, the graph will only show the rows available from the table; if you also check **Show Pie for other**, then a slice for *other* will be shown as zero in the graph and the legend. For example, if you are graphing values for the highest five rows (or four rows with **Show Pie for other** checked), but have only four rows selected in the table, only four rows will be graphed and the slice for *other* will be zero.

---

### Show Pie for Other

When checked, a slice labeled *Other* is added to the graph to show the sum of the values from all of the rows not specifically selected on the Columns tab.

### X-Axis Label, Y-Axis Label, Graph Label

These fields allow entering text titles for the X and Y axes and the title that appears above the graph.

---

**NOTE:** These labels can only be defined when there is a single column selected. However, once the labels are entered, you can select additional columns and retain the same labels.

---

---

## Related Information

For information on related windows:

- [FlexView Properties Window](#)
- [FlexView Bar Graphs](#)
- [FlexView Line Graphs](#)

For information on related tasks:


- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## How to Export a FlexView Catalog

---

You can create a catalog of all or a portion of the FlexViews that have been created for NetSight Console. This feature creates a list of the FlexViews in a selected folder and, if a description was entered as a Note when the FlexView was created, the list also shows the note as a description for the FlexView.

To create a FlexView catalog:

1. Click a FlexView tab in the right panel. If there are no FlexViews in the right panel, pull down the **Tools** menu and select **FlexView > Add FlexView Tab** to add a new FlexView tab. The new tab appears with the default title, *Interface Summary*. Once the tab is added, you can select a specific FlexView and its title will appear on the tab. Click your new FlexView tab.
2. Click the  button on the FlexView toolbar and select **Open** from the menu. A file browser window opens at the default FlexView path.
3. Navigate to the desired FlexView folder and click **Export Catalog**. The catalog will consist of a list of the FlexViews and descriptions within the current folder and its subfolders.
4. Another file browser opens where you can select the target folder where you want to save the FlexView Catalog. The default file format is HTML, which can be viewed using a Web browser.
5. Click Save. The catalog is created. The Open file browser window remains open so that you can select other FlexViews for export if desired.

---

### Related Information

For information on related windows:

- [FlexView Tabs](#)
- [FlexView Properties Window](#)

For information on related tasks:

- [How to Use FlexViews](#)

## How to Export FlexViews to a Web Monitor

---

FlexViews gather information from selected networking devices and display that information in a tabular format. The data can be sorted, filtered, and exported into HTML pages automatically by Console. In addition, each FlexView can be configured to repeat the data gathering at a regular interval (polling). Console allows you to run multiple FlexViews simultaneously, each polling at a specified interval.

These FlexView features provides a foundation for a very powerful web-based monitoring system called a Web Monitor. While Console is running, each active FlexView that has been configured for polling and automatic export will create an updated HTML file at the end of the selected time interval. You can use the Web Monitor to view the data from those HTML files.

Use the following steps to access the Web Monitor, where you will find instructions for configuring FlexViews to export data. You will then be able to view the data using the Web Monitor.

1. In the NetSight Suite Launch Page, click on the Administration tab.
2. Click on the Server Utilities subtab. Enter the NetSight server login credentials.
3. Click on the NetSight Suite Web Monitor link.
4. Instructions for configuring FlexViews to export data are displayed. Follow these instructions to configure your FlexViews and access the data in the Web Monitor.

---

### Related Information

For information on related windows:


- [FlexView Tabs](#)
- [FlexView Properties Window](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)

## FlexView Properties Window

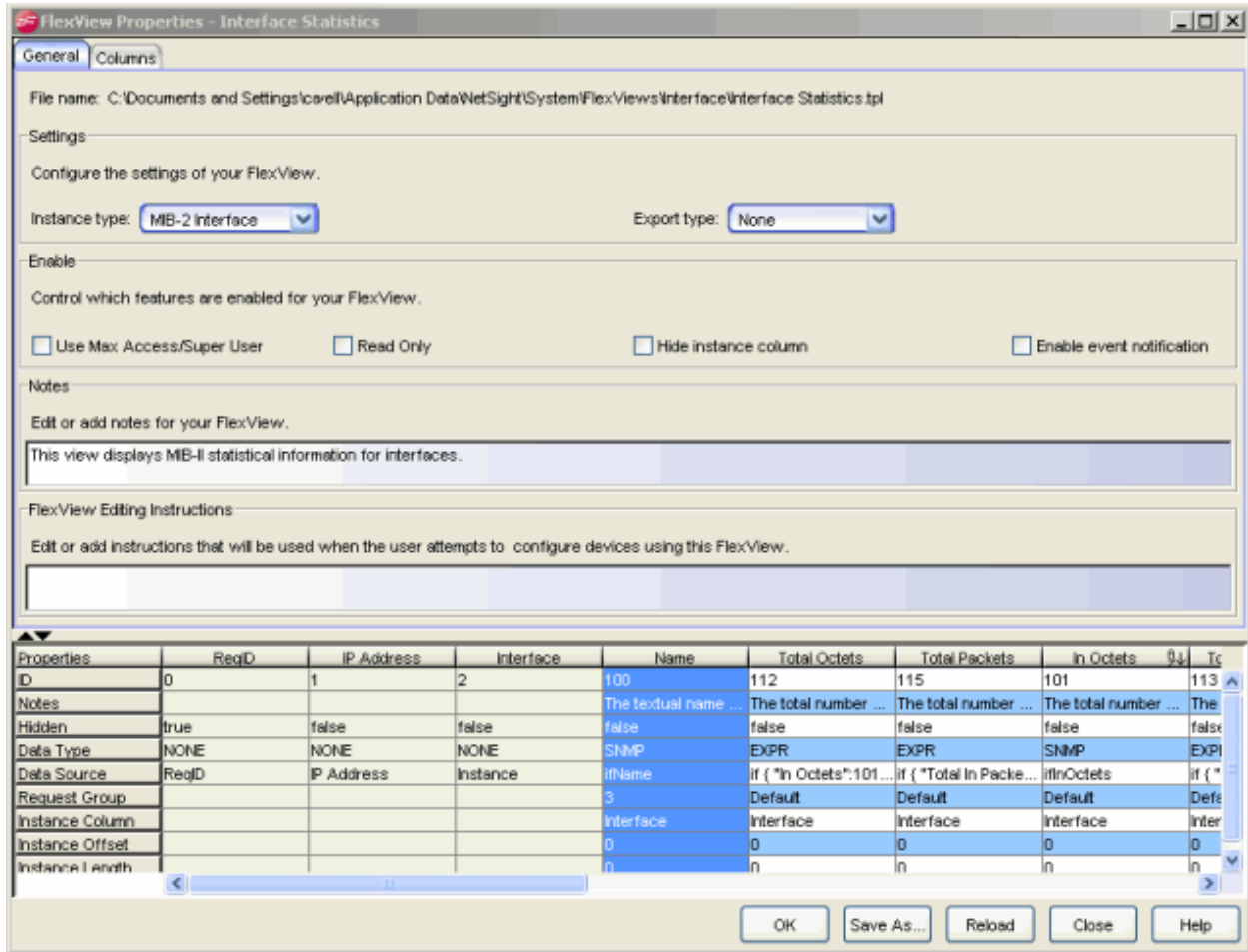
---

You can create a new FlexView or edit an existing FlexView using the FlexView Properties window. To access the FlexView Properties window, click the  (FlexView button) on the FlexView toolbar and select either **New** or **Properties** from the pull-down menu. When opened with the **Properties** menu option, this view contains the settings for the currently selected FlexView. When opened with the **New** menu option, the window contains minimal (default) settings.

The Properties window includes two tabs: the General tab and the Columns tab. This Help topic provides information on how to use these tabs to configure and edit your FlexView.

### General Tab

The General tab is where you can edit FlexView parameters and add any notes to describe its purpose or special conditions. Each field in the window is defined below.



## File name

The name of the file and the path where the this FlexView is saved. When creating a new FlexView, the File name field contains **Untitled** with no path specified.

## Instance type

This setting affects the function and availability of the Port Tools options on the FlexView table right-click menu. The Instance type can be set to **802.1D Bridge Port**, **MIB-2 Interface**, or **Other**.

- **802.1D Bridge Port** - Select 802.1D Bridge Port if the objects in the default request group for this FlexView are instantiated by the MIB object `dot1dBasePort`. The Interface Statistics, RMON Ethernet Statistics, RMON History List, RMON Alarm/Event, RMON Packet Capture, I/F Enable, and I/F Disable options are added to the right-click menu.

- **MIB-2 Interface** - Select MIB-2 Interface if the objects in the default request group for this FlexView are instanced by the MIB Object `IfIndex`. The Interface Statistics, RMON Ethernet Statistics, RMON History List, RMON Alarm/Event, RMON Packet Capture, I/F Enable, and I/F Disable options are added to the menu.
- **Other** - no options are added to the right-click menu.

### Export Type

This setting lets you automatically export FlexView data with each table refresh. Files can be exported as HTML or CSV (spreadsheet compatible) file format. The exported information is saved by default in the `<user's home directory>\AppData\Roaming\NetSight\Console` directory, or you can specify a different export directory in the [FlexView Options](#) (Tools > Options). You can select one of six methods for the exported information:

- **HTML - Replace** - The file is overwritten with each table refresh. The filename is the FlexView name without a timestamp.
- **HTML - Append** - The information in the file is appended with the new information with each table refresh. The filename is the FlexView name without a timestamp.
- **HTML - Timestamp** - A new file is added to the Export directory with each table refresh. The filename incorporates a timestamp of when the data was exported.
- **CSV - Replace** - The file is overwritten with each table refresh. The filename is the FlexView name without a timestamp.
- **CSV - Append** - The information in the file is appended with the new information with each table refresh. The filename is the FlexView name without a timestamp.
- **CSV - Timestamp** - A new file is added to the Export directory with each table refresh. The filename incorporates a timestamp of when the data was exported.

When exported as HTML, this feature makes it possible to use Console to create a Web-based status monitoring system, which allows you to view the status of devices polled by this FlexView from a remote Web browser. Refer to [How to Export FlexViews to a Web Monitor](#) for more information about using this feature to create a Web Monitor.

**Use MaxAccess/SuperUser**

When checked, this FlexView will use the Max Secure or SuperUser passwords for access to retrieve information and set values on devices.

**Read Only**

When checked, the Table Editor is disabled for this table. Writable MIB objects in this table cannot be enforced.

**Hide instance column**

All FlexViews are created with an IP Address column and an Instance column (system-defined) that cannot be removed from the FlexView. However, the Instance Column can be hidden by checking **Hide instance column**.

**Enable event notification**

When checked, the information in the table can be used with the table filter feature to create an alarm for a specific condition. For example, you can select a FlexView that contains columns of various errors and set a filter to show rows that contain greater than zero errors (Type 0 as the filter value, select a column of interest and set the Options for **Match as number** and **Not equal to**). The first time the table contains a row (with the first error), an alarm will be generated and recorded in Console's Event Log. An export file is also created to capture the content of the table when the alarm occurred. The export file defaults to an HTML file and is saved to the `<user's home directory>\AppData\Roaming\NetSight\Exports` directory with the filename, `<FlexView name>_EventData_<date>.html`.

**Edit or add notes for your FlexView**

Use this text field to create a detailed description of this FlexView.

**FlexView Editing Instructions**

Use this text field to provide detailed instructions for how this FlexView should be edited by the FlexView Guided Editor or Table Editor. The information that you provide here will appear at the top of the [Guided Editor window](#).

## Columns Tab

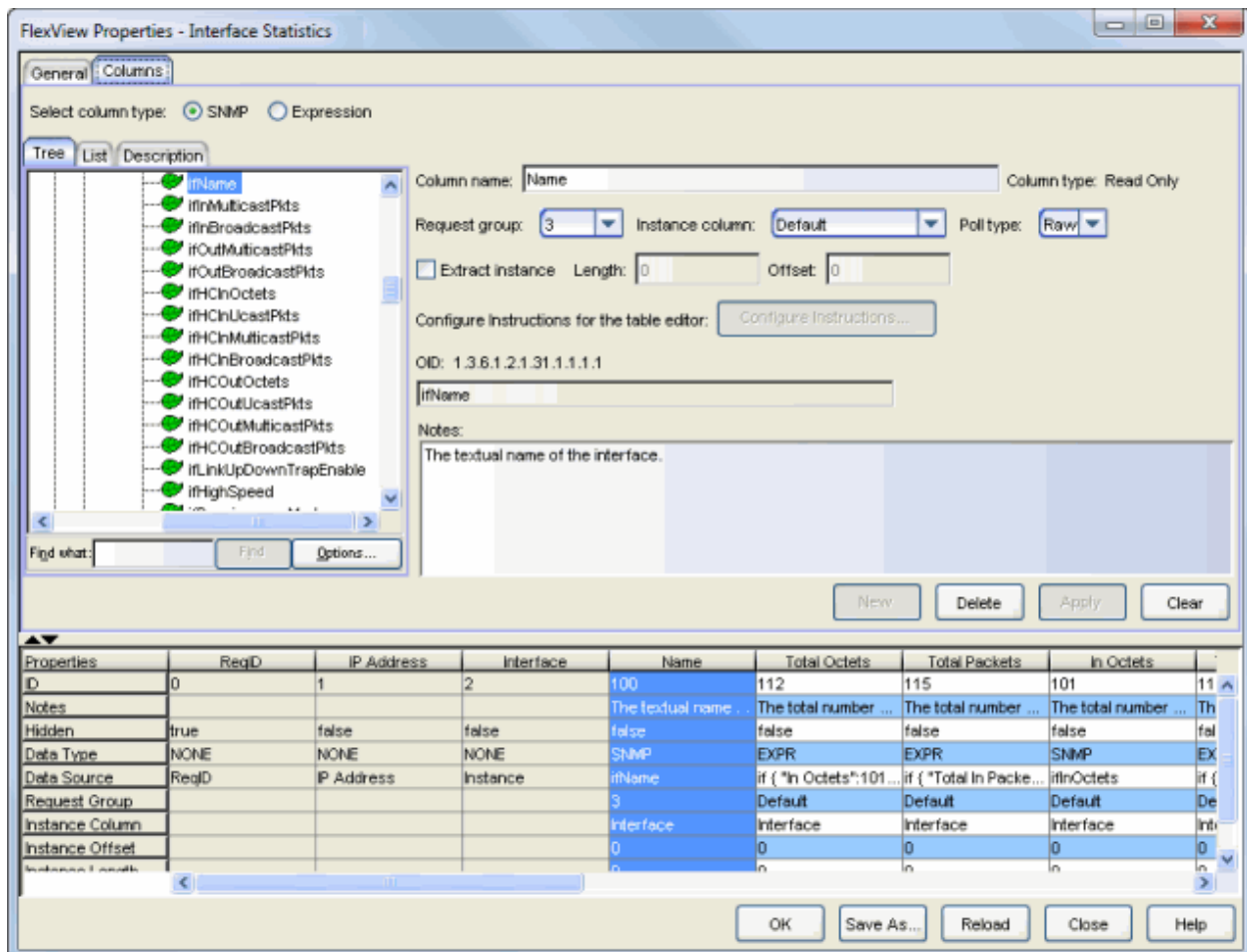
This tab lets you define the content and arrangement of information in your FlexViews. You can define columns that present the values for particular MIB objects or create expressions that combine specific MIB objects, to present information that shows the relationship between those objects. With **SNMP**



selected, the Columns tab lets you configure columns to show the values for specific MIB objects. When **Expression** is selected, the Columns tab becomes an expression editor, providing functions that allow you to combine the values of specific MIB objects.

### Columns Tab - SNMP

With the SNMP column type radio button selected at the top of the tab, the Columns tab lets you add and configure FlexView columns to show the values for specific MIB objects. Each field in the window is defined below.



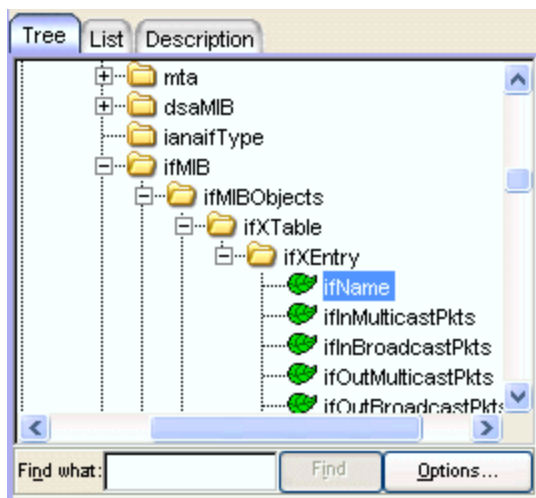
### MIB Object Selector

The MIB Object Selector panel on the left side of the upper panel contains three tabs. The **Tree** and **List** tabs let you select MIB objects for the columns that you are configuring in your FlexView. The **Description** tab shows the text description for MIB objects selected from the MIB Tree or List tab.

## Tree Tab

This tab shows the supported MIBs as a tree hierarchy. You can expand the tree to select MIB objects that you want to appear in your FlexView. Once an object is selected from the tree, you can name the column (Column Name) that will contain this object's value and Add your selection to the list in the FlexView Columns panel. You can search the tree to locate a specific MIB Object by typing all or part of a text string for a particular Object ID or Description into the **Find what** field, selecting an search option, and clicking **Find**. For more information on how to select options, refer to Help on the Find toolbar.

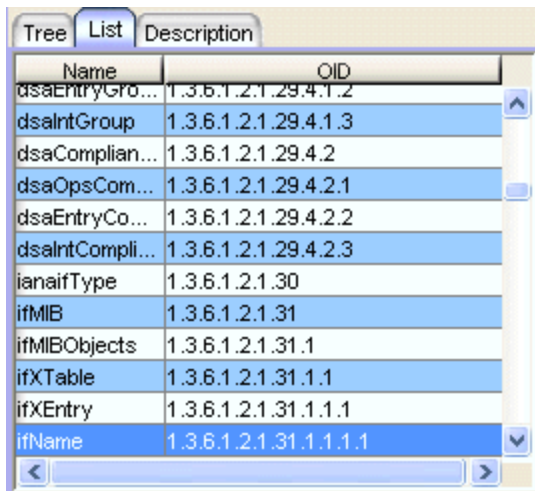
### *Sample Tree Tab*



## List Tab

This tab presents MIB objects in a table. A table right-click menu provides find and filter features to help you locate specific MIB objects. You access these Table Tools through a right-mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools or the Table Settings window Help topic.

### Sample List Tab



Name	OID
dsaEntryGro...	1.3.6.1.2.1.29.4.1.2
dsaIntGroup	1.3.6.1.2.1.29.4.1.3
dsaComplian...	1.3.6.1.2.1.29.4.2
dsaOpsCom...	1.3.6.1.2.1.29.4.2.1
dsaEntryCo...	1.3.6.1.2.1.29.4.2.2
dsaIntCompli...	1.3.6.1.2.1.29.4.2.3
ianaIfType	1.3.6.1.2.1.30
ifMIB	1.3.6.1.2.1.31
ifMIBObjects	1.3.6.1.2.1.31.1
ifXTable	1.3.6.1.2.1.31.1.1
ifXEntry	1.3.6.1.2.1.31.1.1.1
ifName	1.3.6.1.2.1.31.1.1.1.1

### Description Tab

This tab displays the text description (as it appears in the MIB) for a selected MIB object.

### Column Name

This is a name (up to 48 characters) that you assign to the column where the value of this MIB object will be displayed. Enter a name for this FlexView column, then click **Apply** to apply the name to the column.

### Column Type

This field shows the access permitted for the currently selected MIB object (Read Only, Read Write, or No Access).

---

**NOTE:** When FlexView data is retrieved, the data for columns of type *No Access* is extracted from the Instance column.

---

### Request Group

NetSight Console supports multiple SNMP requests. You can assign a particular MIB object to one of four request groups corresponding to a particular grouping of SNMP requests sent to devices. By grouping MIB objects, you can separate requests for objects that may not be supported on a particular device from objects that are. Requests are done according to group order: default, group 2, then group 3 and group 4. For more information, see the [Request Groups](#) and the [Indirect Instancing](#) Help topics.

**Instance Column** (only available with Request Group 2, 3, or 4 selected)

This setting allows using the data returned in the referenced column as the instance for the MIB object selected for this column. The referenced column must be mapped to the **Default** request group or to a request group that has a lower number than the group for the referencing column. For more information, see the [Request Groups](#) and the [Indirect Instancing](#) Help topics.

**Poll Type**

Allows you to set the poll type for the referenced column to:

- Raw - Reports the current value for the MIB object selected for this column.
- Rate - Computes a rate based on consecutive polling samples. This rate can then be used to compute values such as utilization.
- Delta - Computes the difference between the current sample and the last sample.

**Extract Instance**

When checked, this feature allows users having an in-depth knowledge of MIBs to extract data from one instance value and use that data as the instance for retrieving the value of another MIB object. For more information see the [Extract Instance](#) Help topic.

**Configure Instructions**

This button is used when you've selected a writable object for this column. It opens the **Column Instructions** window where you can add text to describe how or why a user may wish to set a particular value for this column. Enter your instructions into the text area and click **OK** to create instructions for this column.

**OID**

This area shows the actual MIB object name for the column being defined.

**Notes**

This area allows you to enter a detailed description for the current column. Enter a note for this FlexView column, then click **Apply** to apply your note.

**New Button**

Adds a new Column Routine to the table using the current definitions in the SNMP Columns tab.

**Delete Button**

Removes the currently selected column from the table.

**Apply Button**

Applies the current definitions to the selected column in the SNMP Columns tab.

**Clear Button**

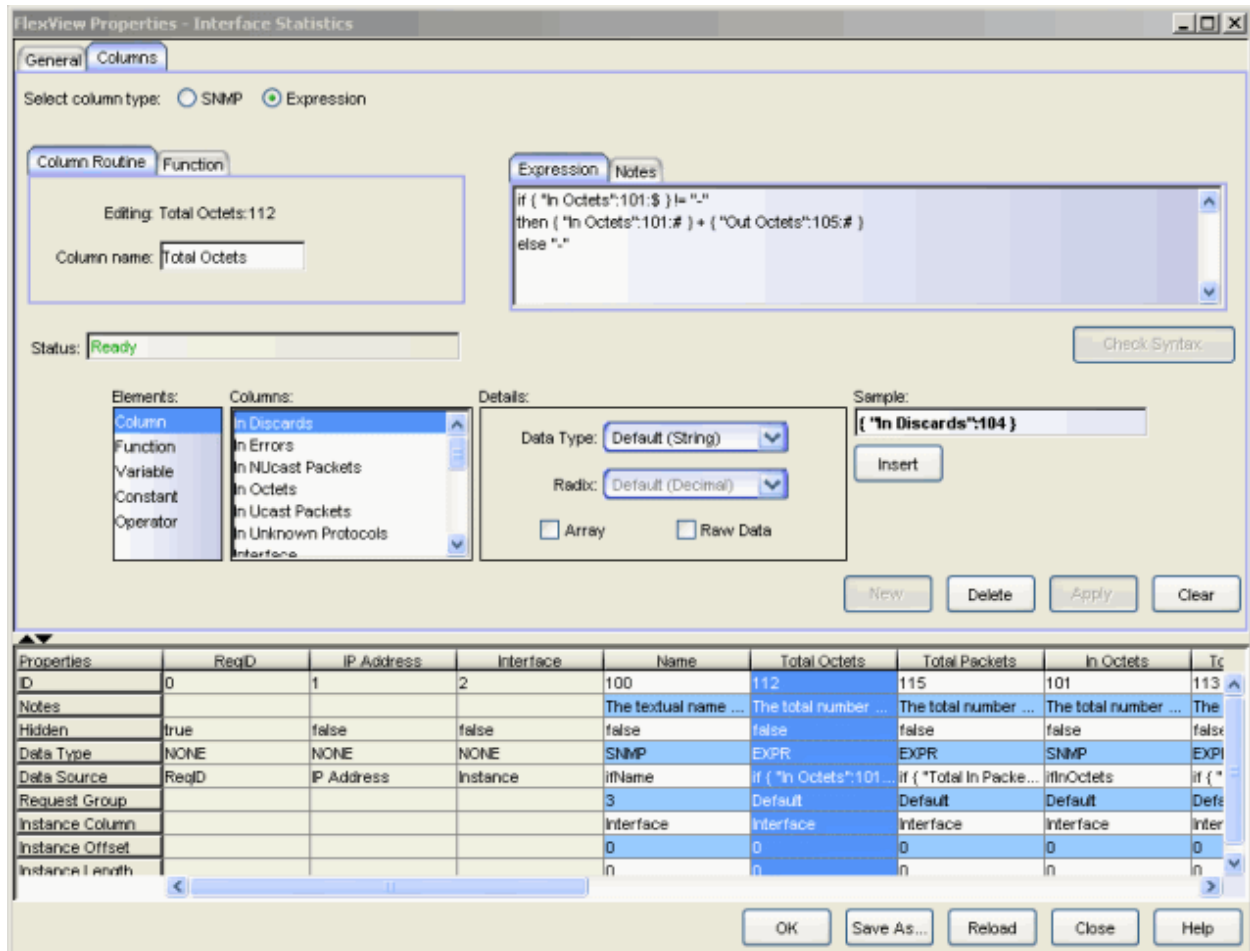
Clears all fields in the SNMP Columns tab.

*Columns Tab - Expression*

The Expression Editor is a powerful tool that lets you enhance the value and clarity of FlexView tables by adding columns that contain data manipulating routines. These routines can access data in other columns in the table, and combine them with data from stored variables, constants, system functions, and user-defined functions to come up with new values to be displayed in the column. A conceptual discussion of the language of the Expression Editor is provided in the [FlexView Concepts - Expression Editor](#) topic.

The Expressions panel is divided into several sub-panels that are used to create an expression. Expressions are assembled in the Expression tab of the panel in the upper right corner of the window. You can type directly into this area or use the [Expression Wizard](#) to construct elements of your expression. The Expression Editor checks for syntax errors when an expression is applied (**Apply**) to a column or function or when the **Check Syntax** button is clicked and the status is displayed in the **Status** field.

### Sample Expression View.



### Column Routine and Function Panel

This panel lets you name routines. Routines are comprised of one or more expressions. There are two types of routines: Column Routines that are associated with a column in the table and Functions. Functions are not associated with a column, but instead, can be referenced from other routines within the table where they were created. Expressions consist of values and operators, where the values can be column references, external routines, stored data, or constants.

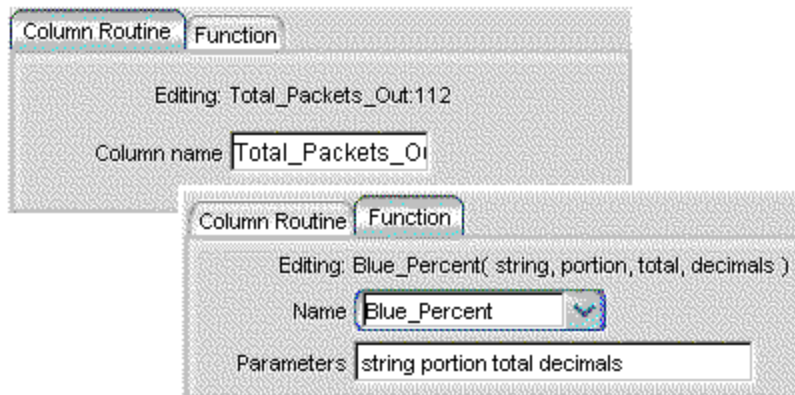
### Column Routine Tab

A column routine is a series of expressions separated by semicolons. This tab lets you name a column routine. This name will appear as the column name for the information produced by this column routine.

## Function Tab

A function is a routine with a name and parameters; but it is not associated with a particular column. This tab lets you enter the name for a function and identify the parameters that the function will take when you use it in a routine.

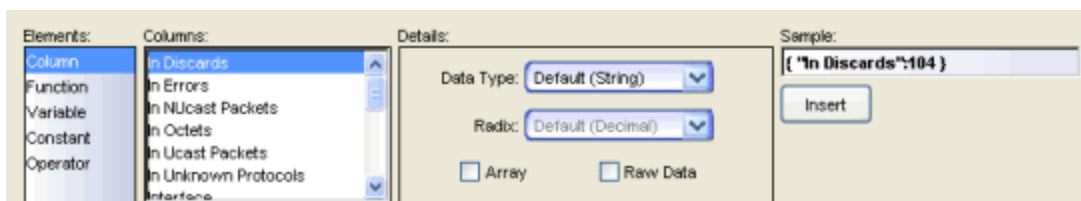
### *Sample Column Routine and Function Tab*



## Expression Wizard

The Expression Wizard consists of four panes that let you choose and define a variety of elements (references) that are used in expressions. The Elements pane lets you select a particular reference element. Working left to right, your selection in the Elements pane determines the selections available from the next pane. For example, when Constant is selected in the Elements pane, you are given choices of the type of constant (string, decimal, hexadecimal, etc.) in the Categories pane. The center pane displays the available columns or operation categories. The right panel lets you define specific details of the selected reference element. As a particular reference element is constructed, it appears in the Sample field. When it is completed, the **Insert** button adds it to the Expression tab at the location determined by the entry cursor. You can click anywhere within an expression to set the position of the entry cursor prior to clicking Insert. The information in the Sample field is constantly checked and the Insert button is active when a valid reference element (consistent with the settings in the wizard) is available to be inserted in the expression.

### *Sample Expression Wizard*



## Elements

### Column

When Column is selected in the left (*Elements*) pane, the center (*Columns*) pane lists the columns for this table. When a particular column is selected, the right (*Details*) pane lets you select/modify the **Data Type** and **Radix** and define the column as an **Array**, or **Raw Data**. You should set these parameters based on the MIB object selected and how it will be used in your expression.

- **Data Type**

This determines the data type that the contents of the column is converted to when being read out of the column.

- **Default (String)** - When no other type is specified the data type defaults to String. However, the element doesn't contain a dollar sign (\$) to explicitly indicate the type.
- **String** - Character string.
- **Integer** - Whole number, without a decimal point.
- **Float** - Number with decimal point or expressed with an exponent.
- **Boolean** - True or False
- **Port List** - A ones and zeros array of ports, separated by colons to indicate operational status of ports numbered 0 through  $n$ .

- **Radix**

The Radix sets the number base (Hexadecimal, Octal, Decimal, Binary) when the data type is set to Integer. This option is disabled for all other data types.

- **Array**

Click Array when the data is in an array format, as in the case of OID, instance, OCTET STRING, IP Address, etc.

- **Raw Data**

Click Raw Data to present the information, unformatted, as it is received from the device.

## Function

Functions are divided into two categories: Table and System. The **Table** folder contains functions that you have created in the Functions tab of the [Column Routines-Functions](#) panel. The System folder contains the following common functions that are provided for your use to manipulate data for a column.



- **Runtime Information**

- **DeltaTime** - Returns a value that is the interval (in the specified *units*) between a *start* and *end* time. The format of a time value conforms to the DateAndTime TEXTUAL-CONVENTION as defined in snmpv2-TC (YYYY-MM-DD, hh:mm:ss.d,Z - year, month, day, hour, minutes, seconds, deciseconds (tenths), timezone. The units parameter is a single case-sensitive character string:
  - "Y" - Years
  - "M" - Months
  - "W" - Weeks
  - "D" - Days
  - "h" - Hours
  - "m" - Minutes
  - "s" - Seconds
  - "d" - Deciseconds (1/10ths)
  - "c" - Centiseconds (1/100ths)
  - "u" - Milliseconds (1/1,000ths)

When units is not specified, the default *units* is centiseconds. When only one time is specified, it is assumed to be the *start* and the current local computer time is used as the *end*. The number of centiseconds between the two times is returned. If the *start* is later than the *end*, a negative number is returned.

- **DeviceType** - For a given IP Address, returns the Device Type as stored in the database and defined in deviceTypes.properties.
- **DisplayName** - Displays either IP Address, sysName, or NickName corresponding to this *IP Address*, according to the current setting for Display Name in the Options. If the device isn't currently in the database, the field will be left blank.
- **SystemName** - Searches the database to find the System Name corresponding to this *IP Address* and displays that value. If the device isn't currently in the database, the field will be left blank.
- **SystemDescriptor** - Searches the database to find the System Description corresponding to this *IP Address* and displays that value. If the device isn't currently in the database, the field will be left blank.

- **NickName** - Searches the database to find the Nickname corresponding to this *IP Address* and displays that value. If the device isn't currently in the database, the field will be left blank.
- **Formatting** - lets you insert a colored icon in the column, select a color for the data, and establish the format for values that appear in the column. Icon and Text attributes are produced by appending hidden code to a string and therefore, you should not perform other string functions on the results of these functions.
  - **BlueIcon, GreenIcon, RedIcon, YellowIcon** - Inserts a ball icon for the selected color before the *string* text.
  - **BlueText, GreenText, RedText, YellowText** - Presents the *string* text in the selected color.
  - **CreateInstance** - Converts a string to its numerical ASCII equivalent for use in an OID Instance.
  - **FormatNumber** - Inserts commas to the left of the decimal point in a (long) *number* and rounds to the number decimal places specified by *decimals*. The *decimals* parameter is the maximum number of digits to the right of the decimal point; the result may be shorter.
  - **FormatTime** - Takes a *number* and an optional *units* string and returns the number as a measurement of time. The units parameter is a single case-sensitive character string: "c" - Centiseconds (1/100 of seconds), "s" - Seconds, "m" - Minutes, "h" - Hours, "d" - Days. When units is not specified, the default *unit* is centiseconds. For example, using the FormatTime function to show 2,000,000 centiseconds:  
FormatTime( 2.0e6 ) Returns 0 Days 5:33:20.00 and 2,000,000 seconds  
FormatTime( 2.0e6, "s" ) Returns 23 Days 3:33:20.00
  - **Magnitude** - Converts the original *number* to K (kilo), M (mega), or G (giga). The optional argument, *decimals*, specifies the number of decimal places in the result. The optional *suffix* (in quotes) lets you refine the magnitude label of your choosing (for example, adding "b", will display the value with Mb).
  - **ParseInstance** - Converts an ASCII string, in instance format, to a text string. Specifying the optional value of *start* will start the conversion at the index specified. *length* defines the length of the converted string.
- **String Manipulation** - lets you format and extract characters from within a string.

- **StringLength** - Returns the length of *string* as a count of the characters.
- **UpperCase, LowerCase** - Converts all of the characters in the *string* to the selected case.
- **Index** - Returns the index of the location of the first occurrence of the specified *character* in the *string*. If the character is not found, returns -1. If a string is used as the *character* parameter, only the first character of the string is used in the search.
- **Contains** - Scans a *string* for *search*. If found, returns the position of the first character in search. If not found, returns -1.
- **Last Index** - Returns the index of the location of the last occurrence of the specified *character* in the *string*. If the character is not found, returns -1. If a string is used as the *character* parameter, only the first character of the string is used in the search.
- **Substring** - Returns a new string that is a sub-string of *string*. It starts at the index, *start*, and stops at *end*. For example Substring ("0123456789", 2, 7) will return "23456". This function is zero-based. If *start* is < 0, > *StringLength*, or not specified the *start* parameter defaults to 0.
- **Mathematical** - lets you operate on integers and floats.
  - **Max** - Returns the larger of two values, *floatA* or *floatB*. If the values are equal, it will return that value. If either value is null or empty, it will return null.
  - **Min** - Returns the smaller of two values, *floatA* or *floatB*. If the values are equal, it will return that value. If either value is null or empty, it will return null.
  - **Percent** - Returns the result of *portion* divided by *total*, carried out to the number of *decimals* and followed by a percent sign (%). The result is rounded, depending on the number of decimals defined. If *total* = 0, Percent will return a divide by zero error.
  - **Power** - Returns a value of *base*, raised to the power of *power*.
  - **Round** - Returns the closest whole number to *float*.
  - **SquareRoot** - Returns the positive square root of *float*.
- **Array Manipulation**
  - **ArrayLength** - Determines the length of the given *array*. If the variable is not an array, returns zero (0). Otherwise, it gives the length of the array, not the index of the last item.

- **isArray** - Determines whether the given variable (*array*) is an array and returns true or false.

## Variable

When Variable is selected from the Elements pane, the Categories pane lets you choose between System and Table Variables. System Variables are not available with this release of Console. When they become available, they can be used in any table. Table Variables are variables that you have created for the current table. They can only be used in the table where they were created. The **Variable** (right) pane allows defining the variable.

A variable consists of a name, optionally followed by an array index in square brackets and an assigned value (of any data type). Variables can be used either as a single value or as an array of values. Variable values are assigned using any of the assignment operators (`=`, `+=`, `-=`, `*=`, `/=`, `%=`, `&=`, `^=`, and `|=`). Variables take on the data type of the value being assigned to it. If a particular variable is assigned more than once in an expression, then the value for the variable is whatever the last assignment sets as the value.

Variables that are assigned as an array use the optional square brackets(`[]`) to specify an array index. All elements in an array must share the same data type. However, the array index does not need to be the same data type as the array elements. An array index can be any expression and the expression can return any data type; it does not have to be an integer. If a particular variable is assigned more than once in an expression, first as an array, then is later as a single value, then the array is overwritten and the variable becomes a single-value (non-array) variable.

## Constant

When Constant is selected in the Elements pane, the Categories lets you choose the data type for a constant. The **Value** (right) pane allows defining the value for the constant.

Each data type has a method of entering constants:

- **Floats** - are a series of decimal digits starting with a non-zero digit. Floats can have an optional decimal point and an optional exponent. For example **23.6e-12**. Plus (+) and minus (-) signs are treated as a unary operators.
- **Integers** - can be expressed as Decimal, Octal, or Hexadecimal. Plus (+) and minus (-) signs are treated as a unary operators.
  - Decimal integers - are a series of decimal digits starting with a non-zero digit. For example, 239.

- Octal integers - are a series of octal digits starting with a zero. For example, 0177.
- Hexadecimal - are a series of hexadecimal digits starting with zero-x (0x). For example, 0x3e4. Hexadecimal digits (A-F) are case independent.
- **Booleans** - are either true or false. Booleans are not case-sensitive.
- **Strings** - are a series of any printable ASCII characters enclosed within double quotes. Double quotes ("), used within a string constant, must be preceded by a back-slash (\). For example, "This is a string constant containing a \"quoted\" word." Likewise, when a backslash (\) appear in a string, it too must be preceded by another backslash. For example "Enter \\ to continue" will be displayed as Enter \ to continue.

## Operator

When Operator is selected in the Elements pane, the Categories lists several groups of operators and the Operators (right) pane lists specific operators.

Operators are used to combine values. Operators are either mathematical or logical, except when using the plus sign to concatenate strings. Operators fall into eight categories: post-unary and pre-unary arithmetic operators, binary arithmetic operators, bit-wise operators, comparison operators, logical operators, conditional operators and assignment operators.

Except for increment and decrement operators, which operate only on integers, all the other operators can work on any value: constants, interim values or variables, function or column references.

Operators fall into eight categories:

- **Post-unary Arithmetic Operators**

There are two post-unary arithmetic operations. Both must be associated with a variable reference since they alter the contents of the value with which they are associated. They operate only on integers.

  - **++** - Increment
  - **--** - Decrement

When these operators are executed, the variable is first converted to an integer, then a new integer value is created with the current value of the expression's variable. This is the value that is returned, because post-increment and post-decrement return the value before the operation. Then

the variable's value is incremented or decremented, and the new integer value is returned to the remainder of the expression.

- **Pre-unary Arithmetic Operators**

There are nine pre-unary arithmetic operators.

- **++** - Increment
- **--** - Decrement
- **+** - Plus or Positive
- **-** - Minus or Negative
- **!** - Not
- **@** - Float-cast
- **#** - Integer cast
- **?** - Boolean cast
- **\$** - String cast

Increment and Decrement must be associated with a variable reference and operate only on integers. When these operators are executed, first the variable is converted to an integer, and then the value is incremented or decremented. Finally, the new integer value is returned to the remainder of the expression.

All of the other Pre-unary operators can be associated with any value.

Plus (+) and Minus (-) operators are associated only with numeric types. If the associated value is an integer or float, the same value is returned but, in the case of negative, with the opposite sign. If the associated value is a boolean or string, a copy of the value converted to an integer is returned but, in the case of negative, with the opposite sign. The positive operator on a numeric type does nothing, but on a non-numeric type it acts the same as integer cast.

The Not operator is associated with boolean values. If the associated value is not a boolean, the value is converted to boolean before the operation is performed.

The cast operators (@, #, ?, \$) return their associated values converted to the cast's data type. Every data type can be converted into every other data type as described earlier.

- **Binary Arithmetic Operators**

There are five binary arithmetic operators:

- **+** - Add
- **-** - Subtract
- **\*** - Multiply
- **/** - Divide
- **%** - Modulo

They operate only on numeric values. Non-numeric values are converted to float or integer before the operation is performed. Either float or integer is returned. For divide and modulo operations, a runtime error will occur if the second value is zero. Refer to the Expression Editor Concepts topic, [Binary Arithmetic Conversion](#) table for implicit conversions during binary arithmetic operations. The only exception to this is the Add operator operating on two string values. When the operator is an add (+) operator, then the non-string operand is cast to a string and the operation is a concatenation of the two strings. The resulting value is a string. If arithmetic addition is required, then the string operand must be explicitly cast to Integer or Float.

- **Bit-wise Operators**

There are three bit-wise operators:

- **&** - Bit-wise AND
- **^** - Bit-wise XOR
- **|** - Bit-wise OR

These operate only on integer values. All non-integer values are converted to integer before the operation is performed. The AND returns a binary one when the corresponding bit position in both numbers are a one. The OR returns a binary one when the corresponding bit position in either or both numbers is a one. The XOR returns a binary one for a particular bit position when the corresponding bit position in either, but not both numbers is a one,

- **Comparison Operators**

There are six comparison operators:

- **<** - Less than
- **<=** - Less than or equal to
- **>** - Greater than
- **>=** - Greater than or equal to

- **==** - Equal
- **!=** - Not Equal

These operate on all data types, but they can only compare the same data types to each other. Strings are lexicographically compared. For booleans, false is less than true. Refer to the implicit conversion table for binary comparison conversions.

- **Logical Operators**

There are two logical operators:

- **&&** - AND
- **||** - OR

They are associated only with boolean values. If either or both values are not boolean they are converted to boolean before the operation is returned. These are used with conditional operators.

- **Conditional Operators**

The **if**, **then**, and **else** operators are used to test a condition and execute one of two expressions, depending on the result of the test. The **if** operator performs the test and, if the condition is true, the expression following the **then** operator is executed. If the condition is false, the expression following the **else** operator is executed. Any expression can follow the **then** and **else** operators. Any expression, except another **if**, **then** or **else** expression, can be used as the condition following the **if** operator. The **else** operator is optional. If the condition being tested is false and there is no **else** operator, an integer zero is returned.

- **Assignment Operators**

There are nine assignment operators:

- **=** Assign
- **+=** Add and assign
- **-=** Subtract and assign
- **\*=** Multiply and assign
- **/=** Divide and assign
- **%=** Modulo and assign
- **&=** Bit-wise AND and assign
- **^=** Bit-wise XOR and assign
- **|=** Bit-wise OR and assign

The



value to the left of all assignment operators must be a variable reference. The assignment operator sets the value and type of the variable reference to the value and type of the second value.

All the other assignment operators, except Assign (=), involve a calculation before the assignment. The manner these calculations are performed is the described in the sections on Arithmetic Operators and Bit-wise Operators. The result of the calculation is then assigned to the variable in the same manner as the assignment operator. The resulting value of any assign is the value assigned. In this manner chained assignments are allowed since they are processed right-to-left. For instance, `index = offset = 0`, the variable `offset` is first assigned the integer value `0`. Since the result of an assignment is the value assigned, the result is `0` which is then used in the assignment of `index`.

## Order of Operations

The following table lists all operators by category to show their order of processing. At the top of the list, Value, is the highest order of processing. Each category takes precedence over the categories below it. For example, given the expression `A == B + 7 * C`, the multiplication of `7` and `C` is done first, then the result is added to `B`, then the new result is compared to `A` for equality.

	Category	Operators
<b>Highest</b>	Value	Column, Function, Variable, Constant, Parenthetical expression
	Post unary	++, --, +, -, !, @, #, ?, \$
	Pre unary	++, --
	Product	*, /, %
	Sum	+, -
	Relative	<, >, <=, >=
	Equality	==, !=
	Bitwise AND	&
	Bitwise XOR	^
	Bitwise OR	
	Logical AND	&&
	Logical OR	
	Assignment	=, +=, -=, *=, /=, %/, &=, ^=,  =
<b>Lowest</b>	Expression	if, then, else

## Parenthetical Expressions

This formula language is hierarchical, which means that operations at a higher level are processed before operations at a lower level. For instance, in the expression  $2 + 3 * 4$ , the multiplication is performed first, even though the addition appears first in the expression. In order to force the addition to be performed first it should appear within parentheses:  $(2 + 3) * 4$ . Any expression can appear in a pair of parentheses, even variable assignments. As many parentheses as is needed can be used; there is no limit to the depth of parentheses. The value and data type returned by the parentheses operators is determined by the result of the last calculation performed in the expression within the parentheses.

## Expression/Notes Panel

### Expression Tab

The Expression tab is the work area where Column Routines and Table Functions are constructed. You can use the Expression Wizard or type directly into the work area. Once you have a Column Routine completed, the Check Syntax button lets you verify that the syntax is correct. This does not guarantee that your routine is logically sound, only that you haven't made any syntax errors.

### Notes Tab

The Notes tab lets you add information about your routine. This information does not appear in the FlexView table.

### Status

This field indicates the state of the Expression Editor and the correctness of the syntax used in expressions. **Ready** indicates that you can enter or edit a routine or a function. The editor checks the syntax of expressions when the **Check Syntax** or **Apply** buttons are clicked. **Passed** indicates that the syntax is correct. The Status field also suggests corrections that are needed when there is a problem with the syntax. Passed does not guarantee that your routine is logically correct, only that there are no syntax errors.

### Insert Button

This button inserts the current entry in the Sample field into the Expression tab work area. The Sample is inserted at the location of the entry cursor.

### Check Syntax Button

Checks the syntax for the current routine. The Status field indicates Passed when the syntax is correct or suggests corrections that are needed. Passed does not guarantee that your routine is logically correct, only that there are no syntax errors.

**New Button**

Checks the syntax for the current routine in the Expression tab and adds a new Column Routine or Table Function to the table. The particular action depends on which tab is selected in the Column Routine/Function panel. This button is active even when there are syntax errors allowing you to create a routine that references a value that has yet to be created.

**Delete Button**

Removes the currently selected column or function from the table. The particular action depends on which tab is selected in the Column Routine/Function panel.

**Apply Button**

Checks the syntax for the current routine and applies it to the selected column or function. This button is active, even when there are syntax errors allowing you to create a routine that references a value that has yet to be created.

**Clear Button**

Clears all fields in the Expression Editor.

## Column Definitions Table

This table shows how the attributes for each of the columns is configured. Every FlexView contains three permanent columns (ReqID, IP Address, and Interface). When creating a new FlexView, this table contains only the three permanent columns. Columns can be repositioned by clicking the heading for a column and dragging it to the left or right.

**OK Button**

Saves the current changes to the FlexView and dismisses the FlexView Properties window.

---

**NOT E:** When re-installing NetSight Console, the installation program saves copies of any FlexViews that you have created/modified in the <install directory>\NetSight\.installer\backup\current\appdata\System\FlexViews folder.

---

**Save As Button**

Opens a file browser window where you can type a name for this FlexView and select a path where the file will be saved.

### Reload Button

Reloads the last saved information for the current FlexView.

### Close Button

Dismisses the FlexView Properties window without saving any changes.

---

## Related Information

For information on related windows:

- [FlexViews \(Interface Summary Tab\)](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## Advanced FlexView Features

---

Users that are familiar with SNMP and the MIBs supported by the devices on their network can create custom FlexViews using some of the more advanced capabilities provided by Console.

Click the links below to learn more about how these features work:

- [Request Groups](#) - let you bundle SNMP requests to improve the effectiveness and performance of your FlexViews.
- [Indirect Instancing](#) - lets you configure FlexViews to use an instance from one MIB table to retrieve data from another MIB table.
- [Extract Instance](#) - lets you extract data from one instance value and use that data as the instance for retrieving the value of another MIB object.
- [FlexView Expression Editor](#) - lets you add columns whose values are the result of executing data manipulating routines.

## FlexView Request Groups

---

NetSight Console uses SNMP requests to retrieve the MIB data that appears in FlexViews. In the interest of performance, Console supports multiple SNMP requests, bundling multiple GET or GETNEXT requests into each SNMP PDU (protocol data unit) when retrieving data for FlexViews. But, the success or failure for a particular SNMP operation is determined at the PDU level. So, when an individual request contained in a PDU fails, the entire PDU is marked as having failed and the data for the requested MIB objects cannot be displayed in the FlexView. This same condition exists when any one of the devices queried supports some, but not all, of the requested MIB objects. The query fails and results in an empty FlexView row being displayed for that device. You could remove the columns for the unsupported MIB objects, but then that data will not be available from devices where those objects are supported.

A better solution would be to assign MIB objects that may not be supported to a separate request. With Console, you can assign MIB objects to one of four request groups (default, 2, 3, or 4) corresponding to a grouping of SNMP requests sent to devices. This feature gives you control over which SNMP requests are bundled into each SNMP PDU. MIB objects that are supported by all devices should be left in one (default) request group and MIB objects that are

supported on some, but not all, devices can be put in a separate request group. If the PDU for the first request group succeeds, but the PDU for the second request group fails, a FlexView row will still be added that contains the data returned in the first PDU. The columns that cannot be populated due to the failure of the second PDU are left blank. Both PDUs will succeed for devices that support all of the objects and the FlexView rows created for those devices will contain valid data in all columns.

When columns are mapped to more than one request group, requests are done according to group order: Default, group 2, group 3, then group 4. Scalar (not contained in a table) and instanced (tabular) MIB data is retrieved by one or more separate SNMP PDUs for each request group. The tabular data usually produces several rows of information for a particular device, one row for each instance in the requested MIB table. When a FlexView is defined to show both scalar and tabular objects, the specific scalar information is repeated for each instance (row) of tabular data returned from a device.

As a general rule, you should:

- assign columns with MIB objects that are supported by all devices to the **Default** request group.
- assign columns with MIB objects that are not supported by all devices to the **2** or **3** request group.

The use of multiple request groups is shown in this example of a network with devices that support three sets of MIB objects.

- Group I supports objects A, B, C, and D,
- Group II supports objects A, B, and C,
- Group III supports objects A, B, and D,

In this example, you would use three request groups to get the FlexView to populate correctly. Since objects A and B are supported by all devices, you can assign columns for A and B to the **Default** request group. Objects C and D are supported by some, but not all devices, so column C should be assigned to request group **2**, and Column D should be assigned to request group **3**.

---

**NOTE:** Utilizing multiple request groups increases the number of SNMP PDUs that must be sent to populate a FlexView.

---

## Related Information

For information on related windows:

- [FlexView Properties Window](#)

For information on related concepts:

- [FlexView Indirect Instancing](#)
- [FlexView Extract Instance](#)
- [FlexView Expression Editor](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## FlexView Indirect Instancing

---

You can configure FlexViews to reference an instance from one MIB table to retrieve data from another MIB table. This feature allows the data returned in the referenced column to be used as the instance for the MIB object selected for this column. The referenced column must have been mapped to the **Default** request group. Indirect instancing uses the **Instance Column** (only available with Request Group 2, 3, or 4 selected) in the FlexView Properties window to specify the particular column that will be used. When indirect instancing is used in a FlexView, additional SNMP requests are assembled to retrieve the instanced data for the selected MIB object.

Request Groups are staged and queried in the following order: default, group 2, then group 3 and group 4 (group 3 and group 4 are sent to the device at the same time). Because of this order, a referenced column must be mapped to a lower group so that the referenced value is valid at the time of the query. For example, **Request Group 2** can only reference the **Default** request group. **Request Groups 3 and 4** can only reference values returned for **Request Group 2** and the **Default** request group.

To see how this feature can be useful, consider the IETF dot1dBridge MIB. This MIB is instanced by dot1dBridgePortIndex. Unfortunately, the Bridge MIB

doesn't contain any objects that describe each port in the bridge. A human readable description for each interface in a device can be found in the Interface Table, but this table is instanced by Interface Index (ifIndex) rather than dot1dBridgePortIndex. Because bridge ports and ifIndices are not mapped one-to-one, objects from the Bridge Table and Interface Table cannot be combined in a FlexView without indirect instancing.

For an example of how Indirect Instancing is used in an actual FlexView, see the "Bridge Port Summary" FlexView in the Bridge folder.

- 
- NOTES:**
1. Console's FlexView logic doesn't assure that data that is obtained from one column and used as an instance in an SNMP GET for another column is a valid instance. There is no checking on the data type or the range of the data to assure that the resulting SNMP GET operation will be meaningful. You should carefully debug and test any custom FlexViews on a variety of devices before relying on the data returned in them.
  2. Request Group 4 cannot use a column in Request Group 3 for instancing. Group 3 and 4 requests are not staged; they are sent to the device at the same time.
- 

Continuing with the example of the dot1dBridge MIB, it turns out that there is a relationship between dot1dBridgePorts and Interfaces. An object contained in the entry for each bridge port (in the Bridge MIB) called the dot1dIfIndex cross-references each bridge port with an entry in the Interface Table. Using indirect instancing, two new columns could be added to any Bridge MIB based FlexView that together allow a description of the interface mapped to each bridge port to be displayed.

The first column, containing the dot1dIfIndex object, would be associated with the default request block. A second column containing the IfDesc object would be assigned to request group 2 or 3 and would have the **Instance Column** setting reference the column containing the dot1dIfIndex.

When data for the new FlexView is retrieved from selected devices, a MIB walk using GETNEXT will first be done (on the bridge mib) to gather the data for all columns associated with the default request block. For each bridge port instance returned from each device, a PDU will be sent containing a GET request for the IfDesc object using the value returned for dot1dIfIndex as the instance for the GET operation. When the data is returned from the device, it will be inserted into the correct row/column of the FlexView. Once the FlexView is defined to your satisfaction, you may want to *Hide* the dot1dIfIndex column from the FlexView display and *Save* the FlexView.



## Related Information

For information on related windows:

- [FlexView Properties Window](#)

For information on related concepts:

- [FlexView Extract Instance](#)
- [FlexView Request Groups](#)
- [FlexView Expression Editor](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## FlexView Extract Instance

---

This feature lets users with an in-depth knowledge of MIBs, extract data from one instance value and use that data as the instance for retrieving the value of another MIB object.

The elements that make up a multi-part instance or other object are formatted as a dot-delimited string (e.g., 1.2.3.4.5.6). The Extract Instance feature uses an **Offset** value to define the starting position within the string and a **Length** value to specify the number of elements to extract.

For example, setting the **Offset** to 3 and the **Length** to 4, will extract the value 3.4.5.6 from the instance, 1.2.3.4.5.6.

Extract Instance can be used two ways:

- You can use Extract Instance to extract a value from the instance of one MIB object and use that value as the instance to retrieve data from another MIB object. This is similar to *Indirect Instancing*, except that only a portion of the instance is used (extracted) as an instance when retrieving the data from another MIB object. The Extract Instance feature is only necessary if only part of the instance value is needed as a reference to another column.

- You can also use Extract Instance to put the extracted value directly in a column as data. SNMP operations cannot be completed on a column of type **No Access**, but the data for this column type is usually embedded in the instance. You can check Extract Instance for a column of type **No Access** to present the data extracted from the instance in the column for the No Access object.
- 

## Related Information

For information on related windows:

- [FlexView Properties Window](#)

For information on related concepts:

- [FlexView Indirect Instancing](#)
- [FlexView Request Groups](#)
- [FlexView Expression Editor](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

## FlexView Expression Editor

---

The FlexView Expression Editor lets you add columns whose values are the result of executing data manipulating routines. A routine is a series of *expressions* separated by semicolons. The Expression Editor uses a language to create the expressions that make up these routines. These expressions are similar to expressions defined in the C programming language. It provides a series of data reference types and operators, and system (pre-defined) function calls that can be combined to create routines. Routines come in two flavors: **Column Routines** and **Functions**.

### Column Routines

Column routines can access data in other columns in the table, and combine them with data from stored variables, system functions, table functions, and constants to come up with new values to be displayed in a column. Each Column Routine is associated with a single column of a FlexView table. During

row processing, each column is evaluated to determine the contents of the cell associated with the table's columns. For a column that is using a column routine, the column routine is executed and the final result is displayed as the contents of the cell.

## Functions

A function is a routine that is not associated with a column. Instead functions are identified by name and have parameters that must be specified for it to operate on when it is used in an expression. For example, the system function that determines a percentage (to a specified number of decimal places) is named `Percent` and has three parameters: `portion` which is the numerator, `total` which is the denominator, and `decimal`, which specifies the number of decimal places with which to express the result. Functions come in two flavors: **System Functions** and **Table Functions**. System functions are provided with Console and can be used in any FlexView table. Table Functions are functions that you create, but they can only be used within the table where they were created.

## *The Language of FlexView Expressions*

FlexView Expressions consist of elements that are capable of referencing other columns in a FlexView Table and, using a format that is conducive to the needs of a routine, casting values into whatever data type is necessary and manipulating the data both as single values and as arrays.

## Expressions

As stated earlier, a routine consists of one or more expressions, separated by semicolons. And, an expression consists of one or more *values* combined using operators. Every expression returns a value when it completes its processing. The value of the final expression of a routine is the value of the routine.

- Expressions may call a system function or table function, treating it as a value. The function executes when an executing column routine calls it. The function returns a value which is used as a value in the calling expression.
- Expressions may be assigned to variables.

These are all examples of expressions:

```
total = {"sent":108:#} + {"received":109:#} + {"errors":110:#}; // Add
three columns and
```

```
percent = ( if total != 0 then #{sent} / total else 0 ); // Don't do the
divide if total is zero

FormatFloat( percent, 5, 2 ) + "%"; // Format percent and append a %

x = ( - b + SquareRoot( b * b + 4 * a * c ) ) / ( 2 * a ); // Equation using
3 variables: a, b & c

"Router"; // A single value is an expression
```

---

**NOTE:** Expressions can be commented using double slashes (//) and all text between the double slashes and the end of a line is ignored for execution.

---

## Values

Values are either *explicit* or *implicit*. Explicit values are entered into an expression and processed when the expression is executed. Explicit values are expressed as constants, variable references, column references, and function references. Implicit values are the result of interim calculations and references that are passed along to the next step in the expression execution. For instance, in the expression **\$result + "%"**, first the variable **result** is evaluated. Then it is cast to a string (**\$** is the string casting operator), which creates an interim value and finally, this interim value is concatenated with the string constant **"%"** to create a new interim value, which is the final **result** (value) of the expression. All values are expressed as a *Data Type*.

## Data Types

There are four data types: float, integer, boolean, and string. The data type for a value is determined when a value is created or, in the case of variables, the variable is assigned. All operators work on one or more data types. If a value does not have the data type expected by an operator, the value is converted to the correct data type. Values can be explicitly **cast** (converted) to a specific data type to insure the correct processing of the data. There are casting operators that can be used at any point in a calculation to force the result of all or part of a calculation to the specific data type.

---

**NOTE:** Console implements a Float as a Java *double* and an Integer as a Java *long*. Therefore their respective ranges are the same as Java.

---

## Casting

Casting converts one data type to another. There are four data type casting operators:

- @ - Float
- # - Integer
- ? - Boolean
- \$ - String

Values can be explicitly cast to a new data type to insure the proper processing of the value. For instance \$count returns the contents of the variable named count cast to a string. This does not change the data type of count. It merely passes the interim value on as a string when that element in the expression is evaluated. Values are also implicitly cast during operations. Any data type can be converted to any other data type, although this may result in data loss.

### *Explicit Conversions*

- **Converting to an Integer**
  - **from a Float** - If the value of the Float is outside of the range of an Integer, it will be set to the maximum or minimum value of an Integer, whichever is closer. The portion of the number to the right of the decimal point is lost.
  - **from a String** - The String is scanned from the beginning for decimal numbers. Scanning stops at the first non-digit character, and the portion scanned is converted. If the value is outside of the range of an Integer, it will be set to the maximum or minimum value of an Integer, whichever is closer. The remainder of the String is lost.
  - **from a Boolean** - True converts to one, and false to zero.
- **Converting to Float**
  - **from an Integer** - The number is converted. Since the range of Integer is a subset of Float, there can be no data loss.
  - **from a String** - The String is scanned from the beginning for numbers that fit the standard notation for floating-point numbers. For example "-123.45e+17". Scanning stops at the first character that falls outside this definition, and the portion scanned is converted. If the magnitude of either the mantissa or the exponent is outside of the range of a

Float, they will be set to their respective maximum or minimum values, whichever is closer. The remainder of the String is lost.

- **from a Boolean** - True converts to one, and false to zero.
- **Converting to String**
  - **from an Integer** - A series of decimal digits is put into the String with no leading zero except in the case of zero.
  - **from a Float** - A series of decimal digits followed by a decimal point, and optionally followed by one or more decimal digits is put into the String. No leading or trailing zeroes will be put into the string, except in the case of zero.
  - **from a Boolean** - TRUE or FALSE is put into the String.
- **Converting to Boolean**
  - **from an Integer** - Zero converts to false, all others to true.
  - **from a Float** - Zero converts to false, all others to true.
  - **from a String** - T, TRUE Yes", Y, OK, (case independent) and 1 convert to true, all others to false. Comparisons are case independent.

*Implicit Conversion*

The following tables show implicit conversions from one data type to another.

**Binary Arithmetic Conversions**

This table shows the data types returned for binary arithmetic operations involving types X and Y. This applies to addition (+), subtraction (-), multiplication (\*), division (/), modulo (%), and all assignment operations that perform these arithmetic operations (+=, -=, \*=, /=, and %=).

The ➡ symbol indicates which operand will be converted to what data type and what the resulting data type will be. For example, **X ➡ Float** indicates that the X value is cast to a Float and Float will be the result of the operation.

<b>x</b>	<b>y</b>	<b>Float</b>	<b>Integer</b>	<b>Boolean</b>	<b>String</b>
<b>Float</b>		Float	Y ➡ Float	Y ➡ Float	X ➡ String (see Note)
<b>Integer</b>		X ➡ Float	Integer	Y ➡ Integer	X ➡ String (see Note)
<b>Boolean</b>		X ➡ Float	X ➡ Integer	X,Y ➡ Integer	X ➡ String (see Note)
<b>String</b>		X ➡ Float	X ➡ Integer	X,Y ➡ Integer	String

**NOTE:** When one data type is a string and the operator is an addition (+) operator, then the non-string operand is cast to a string and the operation is a concatenation of the two strings. The resulting value is a string. If arithmetic addition is required, then the string operand must be explicitly cast to Integer or Float.

## Comparison Conversions

This table shows the data types used during comparison operations involving types X and Y. The indicated conversion takes place before the comparison. A boolean is always returned. The operators this applies to are equals (=), not equals (!=), greater than (>), greater than or equal to (>=), less than (<), and less than or equal to (<=).

The ➔ symbol indicates which operand will be converted to what data type. For example, **X ➔ Float** indicates that the X value is converted to a Float and a Float comparison will be performed.

	<b>y</b>	<b>Float</b>	<b>Integer</b>	<b>Boolean</b>	<b>String</b>
<b>x</b>					
<b>Float</b>		Float	Y ➔ Float	Y ➔ Float	X ➔ String
<b>Integer</b>		X ➔ Float	Integer	Y ➔ Integer	X ➔ String
<b>Boolean</b>		X ➔ Float	X ➔ Integer	Boolean	X ➔ String
<b>String</b>		Y ➔ String	Y ➔ String	Y ➔ String	String

Data type casting is high in the order of precedence. So, in order to cast the results of a calculation, it would need to be parenthesized. For example  $\$(4+8)$  would do the addition and then cast the result as a string, returning a string of "12". The expression,  $\$4+8$  would cast the 4 to a string, then convert the integer 8 to a string and concatenate 4 and 8 and return the result as the string, "48".

## Constants

Each data type has a method of entering constants:

- **Floats** - are a series of decimal digits starting with a non-zero digit. Floats can have an optional decimal point and an optional exponent. For example **23.6e-12**. Plus (+) and minus (-) signs are treated as a unary operators.
- **Integers** - can be expressed as Decimal, Octal, or Hexadecimal. Plus (+) and minus (-) signs are treated as a unary operators.
  - Decimal integers - are a series of decimal digits starting with a non-zero digit. For example, 239.

- Octal integers - are a series of octal digits starting with a zero. For example, 0177.
- Hexadecimal - are a series of hexadecimal digits starting with zero-x (0x). For example, 0x3e4. Hexadecimal digits (A-F) are case independent.
- **Booleans** - are either true or false. Booleans are not case-sensitive.
- **Strings** - are a series of any printable ASCII characters enclosed within double quotes. Double quotes ("), used within a string constant, must be preceded by a back-slash (\). For example, "This is a string constant containing a \"quoted\" word." Likewise, when a backslash (\) appear in a string, it too must be preceded by another backslash. For example "Enter \\ to continue" will be displayed as Enter \ to continue.

## Operators

Operators are used to combine values. Operators are either mathematical or logical, except when using the plus sign to concatenate strings. Operators fall into eight categories: post-unary and pre-unary arithmetic operators, binary arithmetic operators, bit-wise operators, comparison operators, logical operators, conditional operators and assignment operators.

Except for increment and decrement operators, which operate only on integers, all the other operators can work on any value: constants, interim values or variables, function or column references.

### *Post-unary Arithmetic Operators*

There are two post-unary arithmetic operations. Both must be associated with a variable reference since they alter the contents of the value with which they are associated. They operate only on integers.

- **++** - Increment
- **--** - Decrement

When these operators are executed, the variable is first converted to an integer, then a new integer value is created with the current value of the expression's variable. This is the value that is returned, because post-increment and post-decrement return the value before the operation. Then the variable's value is incremented or decremented, and the new integer value is returned to the remainder of the expression.



### *Pre-unary Arithmetic Operators*

There are nine pre-unary arithmetic operators.

- **++** - Increment
- **--** - Decrement
- **+** - Plus or Positive
- **-** - Minus or Negative
- **!** - Not
- **@** - Float-cast
- **#** - Integer cast
- **?** - Boolean cast
- **\$** - String cast

Increment and Decrement must be associated with a variable reference and operate only on integers. When these operators are executed, first the variable is converted to an integer, and then the value is incremented or decremented. Finally, the new integer value is returned to the remainder of the expression.

All of the other Pre-unary operators can be associated with any value.

Plus (+) and Minus (-) operators are associated only with numeric types. If the associated value is an integer or float, the same value is returned but, in the case of negative, with the opposite sign. If the associated value is a boolean or string, a copy of the value converted to an integer is returned but, in the case of negative, with the opposite sign. The positive operator on a numeric type does nothing, but on a non-numeric type it acts the same as integer cast.

The Not operator is associated with boolean values. If the associated value is not a boolean, the value is converted to boolean before the operation is performed.

The cast operators (@, #, ?, \$) return their associated values converted to the cast's data type. Every data type can be converted into every other data type as described earlier.

### *Binary Arithmetic Operators*

There are five binary arithmetic operators:

- **+** - Add
- **-** - Subtract

- **\*** - Multiply
- **/** - Divide
- **%** - Modulo

They operate only on numeric values. Non-numeric values are converted to float or integer before the operation is performed. Either float or integer is returned. For divide and modulo operations, a runtime error will occur if the second value is zero. Refer to the [Binary Arithmetic Conversion](#) table for implicit conversions during binary arithmetic operations. The only exception to this is the Add operator operating on two string values. When the operator is an add (+) operator, then the non-string operand is cast to a string and the operation is a concatenation of the two strings. The resulting value is a string. If arithmetic addition is required, then the string operand must be explicitly cast to Integer or Float.

### *Bit-wise Operator*

There are three bit-wise operators:

- **&** - AND
- **^** - XOR
- **|** - OR

These operate only on integer values. All non-integer values are converted to integer before the operation is performed. The AND returns a binary one when the corresponding bit position in both numbers are a one. The OR returns a binary one when the corresponding bit position in either or both numbers is a one. The XOR returns a binary one for a particular bit position when the corresponding bit position in either, but not both numbers is a one,

### *Comparison Operators*

There are six comparison operators:

- **<** - Less than
- **<=** - Less than or equal to
- **>** - Greater than
- **>=** - Greater than or equal to
- **==** - Equal
- **!=** - Not Equal

These operate on all data types, but they can only compare the same data types to each other. Strings are lexicographically compared. For booleans, false is less than true. Refer to the implicit conversion table for binary comparison conversions.

### *Logical Operators*

There are two logical operators:

- **&&** - AND
- **||** - OR

### *Conditional Operators*

The **if**, **then**, and **else** operators are used to test a condition and execute one of two expressions, depending on the result of the test. The **if** operator performs the test and, if the condition is true, the expression following the **then** operator is executed. If the condition is false, the expression following the **else** operator is executed. Any expression can follow the **then** and **else** operators. Any expression, except another **if**, **then** or **else** expression, can be used as the condition following the **if** operator. The **else** operator is optional. If the condition being tested is false and there is no **else** operator, an integer zero is returned.

### *Assignment Operators*

There are nine assignment operators:

- **=** Assign
- **+=** Add and assign
- **\_ =** Subtract and assign
- **\*=** Multiply and assign
- **/=** Divide and assign
- **% =** Modulo and assign
- **& =** Bit-wise AND and assign
- **^ =** Bit-wise XOR and assign
- **| =** Bit-wise OR and assign

The value to the left of all assignment operators must be a variable reference. The assignment operator sets the value and type of the variable reference to the value and type of the second value.

All the other assignment operators, except Assign (=), involve a calculation before the assignment. The manner these calculations are performed is the described in the sections on Arithmetic Operators and Bit-wise Operators. The result of the calculation is then assigned to the variable in the same manner as the assignment operator. The resulting value of any assign is the value assigned. In this manner chained assignments are allowed since they are processed right-to-left. For instance, `index = offset = 0`, the variable `offset` is first assigned the integer value 0. Since the result of an assignment is the value assigned, the result is 0 which is then used in the assignment of `index`.

### Parenthetical Expressions

This formula language is hierarchical, which means that operations at a higher level are processed before operations at a lower level. For instance, in the expression `2 + 3 * 4`, the multiplication is performed first, even though the addition appears first in the expression. In order to force the addition to be performed first it should appear within parentheses: `(2 + 3) * 4`. Any expression can appear in a pair of parentheses, even variable assignments. As many parentheses as is needed can be used; there is no limit to the depth of parentheses. The value and data type returned by the parentheses operators is determined by the result of the last calculation performed in the expression within the parentheses.

### Order of Operations

The following table lists all operators by category to show their order of processing. At the top of the list, Value, is the highest order of processing. Each category takes precedence over the categories below it. For example, given the expression `A == B + 7 * C`, the multiplication of `7` and `C` is done first, then the result is added to `B`, then the new result is compared to `A` for equality.

	Category	Operators
<b>Highest</b>	Value	Column, Function, Variable, Constant, Parenthetical expression
	Post unary	++, —, +, —, !, @, #, ?, \$
	Pre unary	++, —
	Product	*, /, %
	Sum	+, —

	Category	Operators
	Relative	<, >, <=, >=
	Equality	=, !=
	Bitwise AND	&
	Bitwise XOR	^
	Bitwise OR	
	Logical AND	&&
	Logical OR	
	Assignment	=, +=, -=, *=, /=, %=, &=, ^=,  =
<b>Lowest</b>	Expression	if, then, else

## Column References

A column reference consists of the column name and column ID for a selected column (separated by a colon), optionally followed by a colon and formatting information, all within curly braces. Formatting parameters determine the **Data Type** that the contents of the column will be converted to when being read out of the column and whether or not it will be in an array format, as in the case of OID, instance, OCTET STRING, IP Address, etc. Formatting also specifies a **Radix** when the data type is a numeric string, such as hexadecimal and whether the value is an **Array**, and whether to use **Raw Data** (the unformatted value returned as it is by the device). Radix format operators are H, O and D for hexadecimal, octal and decimal respectively. Data type format operators are @, #, ? and \$ for float, integer, boolean and string respectively. To indicate that it should be an array, the data type operator should appear in square brackets. For instance [#] is an array of integer. Array elements that are assigned by a column reference are indexed by consecutive integers, from left to right, with the first integer being zero. Delimiters used to separate elements in an array can be a (the first) space, colon, hyphen or period found in the column's contents.

Some examples of column references:

Contents of "Column"	Column Reference	Value Created	Notes
"Extreme Networks"	{column:<ID>:\$}	Single value string	\$ is the default, so {column:<ID>} will produce the same result
"10.20.30.40"	{column:<ID>:D[#]}	Decimal text Array of integer	D is the default, so {column:<ID>:[#]} will produce the same result

Contents of "Column"	Column Reference	Value Created	Notes
"67-E5-9F-32-00"	{column:<ID>:[#]H}	Hexadecimal text Array of integer	Format operators are case insensitive and order independent
"system.sysUpTime.0"	{column:<ID>:[\$]}	Array of string	String is the default data type, so {column:<ID>:[]} will produce the same result

## Variable References

A variable consists of a name, optionally followed by an array index in square brackets and an assigned value (of any data type). Variables can be used either as a single value or as an array of values. Variable values are assigned using any of the assignment operators (=, +=, -=, \*=, /=, %=, &=, ^=, and |=). Variables are not defined as having a data type, but take on the data type of the value being assigned to it. For example, in the single value variable, **var=12**, **var** is the name of the variable, **12** is the value being assigned, and the equals sign (=) assigns the value to **var**. In this case the variable (**var**) takes the data type of **12**, which is an integer. If a particular variable is assigned more than once in an expression, then the value for the variable is whatever the last assignment sets as the value.

Variables that are assigned as an array use the optional square brackets([]) to specify an array index. All elements in an array must share the same data type. However, the array index does not need to be the same data type as the array elements. An array index can be any expression and the expression can return any data type; it does not have to be an integer. If a particular variable is assigned more than once in an expression, first as an array, then is later as a single value, then the array is overwritten and the variable becomes a single-value (non-array) variable.

When assigning a value to a non-array variable using an array index, the variable becomes an array. In this case the data type of the array becomes the data type of the value being assigned. When assigning a value to an existing array, using an array index, then the newly assigned value will be converted to the data type of the existing array. This way all elements of an array will have the same data type, even though their indexes need not be of the same data type.

A variable is only an array if a value is assigned to it using an index. Variables can be referenced as any data type with the variable converting the data to the requested data type. Any variable can be assigned with a value of any data type. It can then be cast to any other data type, although the cast does not alter the contents of the variable. Any data type can be converted to any other data type, but some data loss may occur.

---

**NOTE:** When variables reference a particular array using more than one data type as an index, the array acts more like a Java Hashtable than an array.

---

Array elements assigned by a column reference must always be indexed by consecutive non-negative integer values, with the first being zero. Variables are accessed (read) by placing them in an expression at the point where their value is needed. If a non-array variable is referenced with an array index, the index is ignored. When a value is assigned to an array variable, the variable stores the last index used. This is used when an array variable is referenced without an index; this last index is used as the default.

Here are some examples of assigning values to variables:

<code>count += 23</code>	Add 23 to the variable named count. If count had a string or boolean before this, it has an integer after this.
<code>ipAddress[0] = 10</code>	Set the variable named ipAddress to be an array variable, and add an integer value of 10 indexed by the integer value of 0. If the variable was not an array before this it becomes an array with the data type of integer, and the 0 is stored as the first index. If ipAddress was an array before this assign, but not with a data type of integer, the integer of 10 is converted to the data type of the array and then stored.
<code>offset = ++index</code>	This will change the values of both offset and index. They are converted to integer. offset is left with the value of index after the conversion, but before the increment.
<code>ifTable ["10.20.32.45"] = "XPedition"</code>	This will assign the string "XPedition" to the array variable ifTable. It is indexed by the string "10.20.32.45". If ifTable is already an array variable, but not of data type string, the string "XPedition" is converted to the appropriate data type. This would cause the data to be lost.

A variable created by a column routine or table function can be referenced by any other column routine or table function associated with the same table. System functions cannot reference table variables. Variables created by system functions, called system variables, can be referenced by all column routines and functions.

If a table variable has the same name as a system variable, a table function or column routine will reference the table variable, not the system variable by the same name. The table variable does not overwrite the system variable.

## Function References

A function reference consists of a function name followed by a pair of parentheses. Optionally one or more parameters, separated by commas, can

appear between the parentheses. Each parameter can be any value of any data type, or expression returning any data type. The functions can be a **System** function or a **Table** function.

A Table function is defined by the user, and can be called by other table functions or column routines associated with the same table. A table function is created only from the Column Routine/Function panel in the FlexView Expression Editor.

System functions are pre-defined by Console. Most of the formatting will be done by these functions. Some examples are Substring(), FormatInteger(), FormatFloat(), etc. Non-formatting system functions are also available. Min() and Max() are two examples. A complete list appears in the appendix. All user-defined functions and column routines can call any system function.

Function parameters are names that appear in the function definition's parameter list. These names are substituted by values when the function is called by a function reference. These parameters act like a variable in that they hold values, and can have values assigned to them. However, function parameters are the only variables that can be referenced only by a single routine, and are the only variables to go out of existence once the routine completes. If a function parameter has the same name as another variable, the parameter will be referenced instead of the other variable by the same name. The other variable is not overwritten by the function parameter.

The following table lists the System Functions available with Console:



Category	Name	Arguments	Description
Runtime Information	DeltaTime	start, end, units	<p>Returns a value that is the interval (in the specified <i>units</i>) between a <i>start</i> and <i>end</i> time. The format of a time value conforms to the DateAndTime TEXTUAL-CONVENTION as defined in snmpv2-TC (YYYY-MM-DD, hh:mm:ss.d, Z - year, month, day, hour, minutes, seconds, deciseconds (tenths), timezone. The units parameter is a single case-sensitive character string:</p> <ul style="list-style-type: none"> <li>• "Y" - Years</li> <li>• "M" - Months</li> <li>• "W" - Weeks</li> <li>• "D" - Days</li> <li>• "h" - Hours</li> <li>• "m" - Minutes</li> <li>• "s" - Seconds</li> <li>• "d" - Deciseconds (1/10ths)</li> <li>• "c" - Centiseconds (1/100ths)</li> <li>• "u" - Milliseconds (1/1,000ths)</li> </ul> <p>When units is not specified, the default <i>units</i> is centiseconds.</p> <p>When only one time is specified, it is assumed to be the <i>start</i> and the current local computer time is used as the <i>end</i>. The number of centiseconds between the two times is returned.</p> <p>If the <i>start</i> is later than the <i>end</i>, a negative number is returned.</p>
	DeviceType	IP Address	Returns the Device Type for the IP Address as stored in the database and defined in deviceTypes.properties.
	DisplayName	IP Address	Displays either IP Address, sysName, or NickName corresponding to this <i>IP Address</i> , according to the current setting for Display Name in the Options. If the device isn't currently in the database, the field will be left blank.
	NickName	IP Address	Searches the database to find the Nickname corresponding to this <i>IP Address</i> and displays that value. If the device isn't currently in the database, the field will be left blank.
	SystemDescription	IP Address	Searches the database to find the System Description corresponding to this <i>IP Address</i> and displays that value. If the device isn't currently in the database, the field will be left blank.
	SystemName	IP Address	Searches the database to find the System Name corresponding to this <i>IP Address</i> and displays that value. If the device isn't currently in the database, the field will be left blank.

---

Category	Name	Arguments	Description
	TimeTicks	time	Takes a time returned from the device (e.g. sysUpTime) and converts it to timeticks (1/100th of a second). This is useful for situations where you may want to know if happened within the last 10 minutes (600,000 timeticks).

---

Category	Name	Arguments	Description
Formatting	BlueIcon	string	Adds a Blue icon (ball) before the string text.
	BlueText	string	Colors the string text blue.
	CreateInstance	string	Converts a text string to its numerical ASCII equivalent for use in an OID Instance.
	FormatNumber	number, decimals	Inserts commas to the left of the decimal point in a (long) number and rounds to the number decimal places specified by decimals. The decimals parameter is the maximum number of digits to the right of the decimal point; the result may be shorter.
	FormatTime	number, units	<p>Takes a number and an optional units string and returns the number as a measurement of time. The units parameter is a single case-sensitive character string: "c" – Centiseconds (1/100 of seconds), "s" – Seconds, "m" – Minutes, "h" – Hours, "d" – Days,</p> <p>When units is not specified, the default unit is centiseconds.</p> <p>For example, using the FormatTime function to show 2,000,000 centiseconds:</p> <p>FormatTime( 2.0e6 ) Returns 0 Days 5:33:20.00</p> <p>and 2,000,000 seconds:</p> <p>FormatTime( 2.0e6, "s" ) Returns 23 Days 3:33:20.00</p>
	GreenIcon	string	Adds a Green icon (ball) before the <i>string</i> text.
	GreenText	string	Colors the string text green.
	Magnitude	number, decimals, suffix	Converts to K (kilo), M (mega), or G (giga) based on the original number. The optional argument, decimals, specifies the number of decimal places in the result. The optional suffix (in quotes) lets you refine the magnitude label of your choosing (for example, adding "b", will display the value with Mb).
	ParseInstance	instance, start, length	Converts an ASCII string in instance format to a text string. Specifying the optional value of start will start the conversion at the index specified. length defines the length of the converted string.
	RedIcon	string	Adds a Red icon (ball) before the string text. (Note 1)
	RedText	string	Colors the string text red. (Note 1)
	YellowIcon	string	Adds a Yellow icon (ball) before the string text. (Note 1)
	YellowText	string	Colors the string text yellow. (Note 1)

Category	Name	Arguments	Description
<b>String Manipulation</b>	Contains	string, search	Scans a string for search. If found, returns the position of the first character in search. If not found, returns -1.
	Index	string, character	Returns the index of the location of the first occurrence of the specified <b>character</b> in the <b>string</b> . If the character is not found, returns -1. (Note 3)
	LastIndex	string, character	Returns the index of the location of the last occurrence of the specified character in the string. If the character is not found, returns -1. (Note 3)
	LowerCase	string	Converts all of the characters in the string to lower case.
	StringLength	string	Returns the length of string as a count of the characters.
	Substring	string, start, end	Returns a new string that is a sub-string of string. It starts at the index, start, and stops at end. For example Substring ("0123456789", 2, 7) will return "23453". This function is zero-based. If start is < 0, > StringLength, or not specified the start parameter defaults to 0.
	UpperCase	string	Converts all of the characters in the string to upper case.
<b>Mathematical</b>	Max	floatA, floatB	Returns the larger of two values, floatA or floatB. If the values are equal, it will return that value. If either value is null or empty, it will return null.
	Min	floatA, floatB	Returns the smaller of two values, floatA or floatB. If the values are equal, it will return that value. If either value is null or empty, it will return null.
	Percent	portion, total, decimals	Returns the result of portion divided by <i>total</i> , carried out to the number of <i>decimals</i> and followed by a percent sign (%). The result is rounded, depending on the number of decimals defined. (Note 2)
	Power	base, power	Returns a value of <i>base</i> , raised to the power of power.
	Round	float	Returns the closest whole number to <i>float</i> .
	SquareRoot	float	Returns the positive square root of <i>float</i> .
<b>Array Manipulation</b>	ArrayLength	array	Determines the length of the given array. If the variable is not an array, returns zero (0). Otherwise, it gives the length of the array, not the index of the last item.
	IsArray	array	Determines whether the given variable (array) is an array and returns true or false.

---

Category	Name	Arguments	Description
----------	------	-----------	-------------

---

**Notes:**

1. Icon and Text attributes are produced by appending hidden code to a string and therefore, you should not perform other string functions on the results of these functions.
2. If *total*= 0, Percent will return a divide by zero error.
3. If a string is used as the *character* parameter, only the first character of the string is used in the search.

---

## Related Information

For information on related windows:

- [FlexView Properties Window](#)

For information on related concepts:

- [FlexView Indirect Instancing](#)
- [FlexView Request Groups](#)
- [FlexView Extract Instance](#)

For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)

# How To Use NetSight Console

---

The **How To** section contains Help topics that give you instructions for performing tasks in NetSight Console.

## How to Add, Remove, and Delete Devices

---

You can add devices to any group in the left panel using [Discover](#) or by manually adding devices using menu options, drag-and-drop, or copying devices from one group to another. You can remove a device from a specific group or you can delete a device from the NetSight database, thereby removing it from all groups where it is a member. To learn more about Discover, refer to the [Discover Window](#) help.

Instructions on:

- [Adding Devices to a Group](#)
  - [Manually](#)
  - [From a FlexView Table](#)
  - [Copying and Pasting Devices](#)
  - [Dragging and Dropping Devices](#)
- [Removing Devices from a Group](#)
- [Deleting Devices from the NetSight Database](#)

### Adding Devices to a Group

There are several ways to add devices to a group. You can add them manually: drag and drop, copy and paste one or more devices from another device group, or add devices from a FlexView table to a user-created group.

#### *Adding Devices Manually*

1. Click the right mouse button on the group to which you want to add a device and select **Add Device** from the right-click menu. The **Add Device** window opens, where you can define the IP address and Profile for the device being added.
2. Type an **IP Address**.
3. Use the **Profile** drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.
4. If used for this device, specify a **SNMP Context**. An SNMP context is a collection of MIB objects, often associated with a network entity. The SNMP

context lets you access a subset of MIB objects related to that context. Console lets you specify a SNMP Context for both SNMPv1/v2 and SNMPv3.

The use of context differs depending on the protocol version being used with a user's credentials:

- When used, with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.
- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, an SNMPv1 or SNMPv2 community name can be mapped, through Local Management, to a particular SNMP context on the device. Thus, when SNMPv1/v2 credentials are used with a Context entry, access is granted to the subset of MIB objects associated with that credential (community name). If the credential used is accepted, but the context specified doesn't match a context configured on the device, access is granted to the default context.

Console treats each context for a given device (IP address) as a distinct device. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to your device configuration guide for more information about setting and showing SNMP contexts.

5. You can use the default nickname or click **Specify** to assign a unique nickname to this device. The default nickname for SNMP devices is the `sysName` MIB object, or if no `sysName` has been assigned, the device's IP address. The default nickname for pingable devices is the IP address.
6. Click **Apply**. The new device appears in the group and is automatically added to the **All Devices** group.

### *Adding Devices to a Group from a FlexView Table*

To add devices from a FlexView Table to a user-created group in the left panel:

1. If the user-created group to which you want to add the devices does not exist, [add](#) it now.
2. Select or create a FlexView table that lists the devices you want to add to a group.



3. In the table, select the device(s) you want to add to a group. To select multiple non-sequential devices, use the **Control** key. To select multiple sequential devices, use the **Shift** key.
4. Right click the table and select **Add Device to Group** from the right-click menu. The [Add Device\(s\) to a Group window](#) opens.
5. Expand the appropriate group(s) in the group selection panel and select the target group.
6. Click **OK**. The device(s) selected in the FlexView table are added to the target group.

### *Copying and Pasting Devices*

You can copy devices from one group to another. You can even copy an entire device group if that's convenient and paste it into another group to create a sub-group in the target group.

To add devices by Copying and Pasting:

1. In the left panel, expand the group containing the devices that you want to copy.
2. Select the device to be copied.
  - To copy a single device, right click on the device and select **Copy** from the right-click menu.
  - To select multiple devices from the selected group, hold the **Control** key while clicking to select non-consecutive devices or hold the **Shift** key while clicking to select a range of consecutive devices, then right click on one of the selected devices and select **Copy** from the right-click menu.
3. Right click on the group where you are placing the device(s) and select **Paste** from the right-click menu.

To add a group by Copying and Pasting:

1. In the left panel, right click on the group that you want to copy and select **Copy** from the right-click menu.
2. Right click on the group where you are placing the group and select **Paste** from the right-click menu. The group is added as a sub-group, containing all of the devices that were members of the original group.

**NOTE:** When you paste a group, you are actually adding a user-created group and you can only add groups in the My Networks Group or another user-created group.

---

### *Dragging and Dropping Devices*

You can add devices by dragging from one group and dropping into another. You can also drag and drop an entire device group to create a sub-group in the target group.

To add devices by Dragging and Dropping:

1. In the left panel, expand the hierarchy to show the target group and the group containing the devices that you want to add.
2. Select device(s) to be dragged and dropped.
  - To select a single device, click and hold on the device and drag it into the target group.
  - To select multiple devices from the selected group, hold the **Control** key while clicking to select non-consecutive devices or hold the **Shift** key while clicking to select a range of consecutive devices.
3. Click and hold on one of the selected devices and drag them into the target group.

To add a group by Dragging and Dropping:

1. In the left panel, expand the hierarchy to show the target group and the group that you want to add.
2. Click and hold on the group and drag it into the target group. The group is added as a sub-group, containing all of the devices that were members of the original group.

---

**NOTE:** When you paste a group, you are actually adding a user-created group and you can only add groups in the My Networks Group or another user-created group.

---

## **Removing Devices from a Group**

Devices can be removed from user-created groups without deleting the device from the NetSight database. To remove devices from a group:

1. Expand the groups in the left panel to select the device being removed.

2. Click the right mouse button on the device and select **Remove from Group** from the right-click menu. The selected device will be removed without further confirmation.

## Deleting Devices from the NetSight Database

Devices can be deleted from both system-created groups and user-created groups in the left panel. When devices are deleted from the NetSight database they are removed from all groups where they are a member. To delete devices from the NetSight database:

1. Expand the groups in the left panel to select the device being deleted.
2. Click the right mouse button on the device and select **Delete** from the right-click menu. A confirmation message advises that you are deleting the device from the NetSight database.
3. Click **No** to retain the device in the database or click **Yes** to delete the device. The selected device will be deleted without further confirmation.

---

### Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)

For information on related tasks:

- [How to Add, Remove, and Rename Groups](#)

## How to Add and Remove Port Elements

---

You can add ports to the My Network or to any user-created group by choosing **Add Port Elements to Group** from the right-click menu in a FlexView table. You can remove a port from a specific group, or you can delete the port from the NetSight database, thereby removing it from all groups where it is a member.

Instructions on:

- [Adding Ports to a Group](#)
  - [From a FlexView Table](#)
  - [Copying and Pasting Ports](#)
  - [Dragging and Dropping Ports](#)
- [Removing Ports from a Group](#)
- [Deleting Port Elements](#)

### Adding Ports to a Group

There are several ways to add ports to a group. You can add selected ports from a FlexView table, drag and drop them in the tree, or copy and paste one or more ports from another group.

#### *Adding Selected Ports From a FlexView Table*

1. Open a FlexView for the device(s) containing the port(s) that you want to add and click the **Retrieve** button.
2. Click the right mouse button on the port(s) that you want to add to a particular group. The [Port Group Selection](#) window opens.
3. Expand the tree and select the group where the selected port(s) will be placed.
4. Click **Ok** to confirm your choice and close the window. The ports are added to the selected group and to the **All Port Elements** folder.

You can now select specific ports and use FlexViews to query information about those specific ports. You should use the appropriate FlexView to view the type of port being queried. Use a FlexView that is appropriately instanced for the specific port being queried.

For example:

<b>If you create the port element from:</b>	<b>The Port Element contains:</b>
IF instanced FlexView	IF instance
dot1d instanced FlexView	Bridge Port instance and, if available in the table, IF instance
<i>other</i> instanced FlexView	The instance value

### *Copying and Pasting Devices*

You can copy ports from one group to another.

To add ports by Copying and Pasting:

1. In the left panel, expand the group containing the ports that you want to copy.
2. Select the port(s) to be copied.
3. Right click on the port and select **Copy** from the right-click menu. To select multiple ports, hold the **Control** key while clicking to select non-consecutive ports or hold the **Shift** key while clicking to select a range of consecutive ports, then right click on one of the selected ports and select **Copy** from the right-click menu.
4. Right click on the group where you are placing the port(s) and select **Paste** from the right-click menu.

### *Dragging and Dropping Ports*

You can add ports by dragging from one group and dropping into another.

To add ports by Dragging and Dropping:

1. In the left panel, expand the hierarchy to show the target group and the group containing the port(s) that you want to add.
2. Select port(s) to be dragged and dropped.
  - For a single port, click and hold on the port and drag it into the target group.
  - To drag and drop multiple ports, hold the **Control** key while clicking to select non-consecutive ports or hold the **Shift** key while clicking to select a range of consecutive ports. Click and hold on one of the selected devices and drag them into the target group.

## Removing Ports from a Group

Ports can be removed from user-created groups without removing them from the All Port Elements group:

1. Expand the groups in the left panel to select the port being removed.
2. Click the right mouse button on the port and select **Remove From Device Group** from the right-click menu. The selected port will be removed without further confirmation.

## Deleting Port Elements

Use these steps to delete a port from the All Port Elements group and any user-created group where it was a member:

1. Expand the groups in the left panel to select the port being removed.
  2. Click the right mouse button on the port and select **Delete Port Element** from the right-click menu. The selected port element is deleted without further confirmation.
- 

### Related Information

For information on related windows:

- [Port Group Selection Window](#)
- [Main Window](#)
- [Left Panel](#)

For information on related tasks:

- [How to Add, Remove, and Rename Groups](#)

## How to Add MIBs to Extreme Management Center

---

In order to communicate with your network devices, Extreme Management Center (Management Center) relies on a database of compiled MIB information. This database gives Management Center the ability to query and set (as appropriate) MIB objects resident on your devices.

If you want to use Management Center to manage devices other than Extreme Networks devices, you can add the appropriate proprietary MIBs to the MIB database on the Management Center Server. This MIB information is then distributed to the Management Center remote clients. The MIBs for these devices must be compiled prior to being added to Management Center's MIB database. You can run **snmptranslate** to verify the format for MIBs you add to Management Center.

**snmptranslate** is an application that translates one or more SNMP object identifier values from their symbolic (textual) forms into their numerical forms (or vice versa). As described here, snmptranslate is being used only to verify that a MIB has been properly compiled and can be interpreted by Management Center. It attempts to read a particular known MIB object and, if successful, return a brief message.

Management Center provides four scripts that run the snmptranslate tool:

- checkServerMibs.cmd - Windows Management Center Server
- checkMibs.cmd - Windows Management Center client
- checkServerMibs.sh - Linux Management Center Server
- checkMibs.sh - Linux Management Center client

Use the following steps to add a MIB to the MIB database on the Management Center Server.

---

**NOTE:** These steps recommend that you begin by adding your MIBs to the MyMibs directory on the Management Center client. This allows you to test the MIBs without impacting other Management Center clients. You can then add the MIBs to the MyMibs directory on the Server host system. The MIB information is then distributed to the Management Center remote clients.

---

1. With Management Center and MIB Tools shut down, add the new MIB file to:

**Windows 7:** C:\Users\  
name>\AppData\Roaming\NetSight\System\mibs\MyMibs  
**Linux:** ~\NetSight\System\mibs\MyMibs

---

**NOTE:** For Windows 7, the Management Center install defaults to the "Roaming" directory, however it may also be the "Local" directory, depending on how the Domain is set up.

In Windows 7, the MyMibs directory may be hidden. To show hidden files and folders, use the following instructions:

1. Click the **Start** button and open the Control Panel > Appearance and Personalization > Folder Options.
  2. Click the **View** tab.
  3. Click **Show hidden files and folders** in the Advanced Settings section of the window and click **OK**.
- 

2. Use the checkMIBs script to run the **snmptranslate** tool to verify that the MIB you are adding has been properly compiled. The checkMIBs script is located in:

**Windows 7:** C:\Users\  
name>\AppData\Roaming\NetSight\tools\snmputils\checkMIBs.cmd  
**Linux:** ~\NetSight\tools\snmputils\checkMibs.sh

3. If the MIB is correctly compiled, a message similar to the following displays:

```
RFC1213-MIB::sysDescr  
or  
system.sysDescr
```

However, if the MIB is not correctly compiled, the result a series of error messages display. You must correct the discrepancies in the MIB before using it with Management Center. Do not run Management Center with a corrupted MIB. Remove the MIB from the mibs directory prior to starting Management Center or MIB Tools.

4. When you have verified that the MIB is correctly compiled, add the new MIB to the MyMibs directory on the Server host system. The MyMibs directory is saved if Management Center is re-installed and restored



following re-installation. The MyMibs directory lets you maintain your MIBs separately from the MIBs initially installed with Management Center.

```
<install directory>\NetSight\appdata\System\mibs\MyMibs
```

5. Restart the Management Center Server and launch Management Center. The new MIB is automatically distributed to all remote clients.

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)
- [MIB Tools Options Window](#)

## How to Add, Remove, and Rename Groups

---

You can add, remove, and rename user-created groups to the My Network group in the left panel.

### Adding a Group

You can add groups in the left panel under **My Network**, then add/copy devices into these groups to define device groups on your network. You can also create maps to represent the network elements contained within these device groups.

1. Click the right mouse button on the My Network group or on a user-created group to which you want to add a new group and select **Add Device Group** from the right-click menu. The **Add Device Group** window opens.
2. Type a name for your new group and click **Ok** define the name for the new group.

### Renaming a Group

By default, all new groups are named with the designation *New Group* when they are created. You should name your groups as they are created, but you can rename them at any time as follows:

1. Right click on a group and select **Rename Device Group** from the right-click menu. The group name will be highlighted.
2. Place the cursor anywhere in the name, and edit as desired; or, simply begin typing to replace the highlighted text entirely.
3. Press Enter to set your change.

### Removing a Group

You can remove groups that you've created (user-created groups) in the left panel. However, you cannot remove system-created groups. When you remove a group, the devices contained in it are not deleted from the NetSight database. Only the group (container) and any sub-groups within it are removed.

To Remove a group:

1. Expand the groups in the left panel and select the group being removed. Click the right mouse button on the group you wish to remove.
  2. Select Remove from Group from the right-click menu. The selected group will be removed without further confirmation.
- 

### **Related Information**

For information on related windows:

- [Main Window](#)
- [Left Panel](#)

For information on related tasks:

- [How to Add Devices to a Group](#)

## How to Add Third-Party Application Support

---

You can customize the Applications menu in Console and the other NetSight applications to launch third-party applications and/or launch a web browser to display a web page, by editing the ThirdPartyMenu.xml file. You can also edit the ThirdPartyMenu.xml file to perform these functions from the device-level right-click menu. This allows you to run the application or launch a browser by right-clicking a device icon in the Console left-panel tree. You must restart the server before the modified version of the file is deployed to connecting clients.

Use these steps to edit the ThirdPartyMenu.xml file.

1. On the NetSight server system, open the ThirdPartyMenu.xml file. This file is located in the `<install directory>\NetSight\appdata\System\Shared` directory.
2. Edit the file by copying the sample menu list outside the comment tags, and then customizing the menu list to fit your needs. Each application that is added to the menu is defined by a menu element. Valid attributes for a menu element are:
  - **id** - a unique identifier for each menu item.
  - **name** - the text displayed for the menu item.
  - **icon** - an optional icon to identify the menu item. The icon graphic must be placed in the `<install directory>\NetSight\appdata\System\images` directory.
  - **type** - the menu element can be one of two types:
    - **application-menu** - This menu item will be added to the Applications menu in Console and other NetSight applications.
    - **device-menu** - This menu item will be added to the device-level menu in Console only.
3. A menu element may contain one or more application elements or a webpage element. An **application element** has the following valid attributes:
  - **os** - the name of the operating system (in lower case) on which the application will be executed. Only the application corresponding to the host operating system will be executed, so each menu may have

multiple application elements to provide support for different operating systems.

- **name** - a descriptive name for the application.
- **executable** - The fully qualified path name of the executable that will be run when the menu option is selected. Path separators are OS dependent. This path is also client specific. If an executable is not in a location common to all clients, the client version of this file must be updated to the correct path. Otherwise the executable will not run on the client system.

A **webpage element** has only the URL attribute, which is the URL of the webpage to launch in a browser.

4. An application element may also contain multiple "arg" elements, which are arguments passed to the executable. There is only one valid "arg" attribute: "value." The value of the "value" attribute can be anything except for characters that are reserved by XML.
5. The "device-menu" menu type also performs the following conversion on arguments included for each application. An "arg" element whose value is one of the following is automatically converted when the associated executable is run.
  - %IP => IP address of the currently selected device.
  - %SNMP => Maximum available credential for the System Profile mapping. If the device's System Profile is v1 or v2, this would pass the community name in the Profile that is from the highest Access Level's credential. For example, if the Profile only has a Read credential, it would pass that community name. If it has Read and Write credentials, it would pass the community name for the Write credential. If the device's System Profile is v3, this would pass the user and password parameters in the Profile that is from the highest credential.
    1. Auth Priv  
user=user name  
MD5=MD5 password or SHA1=SHA1 password  
DES=DES password
    2. AuthNoPriv  
user=user name  
MD5=MD5 password or SHA1=SHA1 password  
DES=NOT\_SPECIFIED
    3. NoAuthNoPriv  
user=user name

MD5=NOT\_SPECIFIED  
DES=NOT\_SPECIFIED

- %CN => Community Name. This argument provides compatibility with previous releases of NetSight Console. It is equivalent to %SNMP, which should be used instead of %CN.
6. When launching a webpage, the "device-menu" menu type performs the following additional conversions on the URL.
    - %DEVICEIP% = The IP address of the currently selected device. This might be used when the URL is for a page that is served by the device. For example, <http://%DEVICEIP%/Admin>.
  7. Restart the NetSight Server. When you restart the server, the modified version of the file is deployed to connecting clients and the applications will be available on the appropriate menus.

Sample Menu List

```

<menulist id="nsthirdpartymenu" name="NetSight Third
Party">
  <menu id="textEditor" name="NetSight Text Editor"
icon="atlas_icon.gif" type="device-menu">
    <application os="windows" name="Wordpad"
executable="C:\Program
Files\Windows\Accessories\wordpad.exe"/>
    <application os="linux" name="gedit"
executable="/usr/bin/gedit"/>
  </menu>
  <menu id="Telnet" name="NetSight Telnet Window"
icon="conlitel6.gif" type="device-menu">
    <application os="windows" name="CMD"
executable="C:\Windows\System32\cmd.exe">
      <arg value="/K" />
      <arg value="start" />
      <arg value="telnet" />
      <arg value="%IP" />
    </application>
    <application os="linux" name="NetSight
Telnet Window" executable="/usr/bin/gnome-terminal">
      <arg value="-x" />
      <arg value="telnet" />
      <arg value="%IP" />
    </application>
  </menu>
  <menu id="textEditor" name="NetSight Text Editor"
icon="atlas_icon.gif" type="application-menu">
    <application os="windows" name="Wordpad"
executable="C:\Program
Files\Windows\Accessories\wordpad.exe">
    <application os="linux" name="gedit"
executable="/usr/bin/gedit"/>
  </menu>
  <menu id="google" name="Google" icon="application_
go.png" type="application-menu">
    <webpage url="http://www.google.com"/>
  </menu>
</menulist>

```

# How to Assign ACLs to Device Interfaces and Agent Services

---



You can assign ACLs to device interfaces and agent services using the ACL Manager's [interface assignment](#) and [agent assignment](#) views.

Instructions on:

- [Assigning ACLs to Interfaces](#)
- [Assigning ACLs to Agent Services](#)

## Assigning ACLs to Interfaces

Use the following steps to assign an inbound/outbound ACL to a device interface.

1. Select the device in the Console left-panel tree. Click on the ACL Manager right-panel tab.
2. Select the Interface Assignment view using the radio button at the top of the tab.
3. Select the device interface where you want to assign an ACL.
4. Scroll right to see the Inbound ACL and Outbound ACL columns.
5. Click on the Show Table Editor button  to display the table editor row.
6. In the Table Editor row, click on the Inbound ACL or Outbound ACL column to display the ACL Selection window. Expand the folders to select the desired ACL.
7. Click **OK**. A green exclamation mark  marks the cell that has been changed and the Save to Database button becomes active.
8. Click on the Save to Database button to save your change to the ACL Manager Database.
9. Click on the Enforce button to write your changes to the device's active configuration.





**CAUTION:** If the ACL that you are assigning could deny contact with the device from the NetSight server, an error will occur when the device is enforced. There is an Enforce option (Allow ACLs to Deny NetSight) that turns off checking for ACLs which deny access to the device from the NetSight server. Use of this option could result in lost contact with the device. You should **not** apply an ACL that denies access to the device. If contact is denied by an ACL, you must use the device's command line interface (CLI) to remove the ACL and restore contact.

---

## Assigning ACLs to Agent Services

Use the following steps to assign an ACL to an agent service supported on a device.

1. Select the device in the Console left-panel tree. Click on the ACL Manager right-panel tab.
2. Select the Agent Assignment view using the radio button at the top of the tab.
3. Select the agent service where you want to assign an ACL.
4. Click on the Show Table Editor button  to display the table editor row.
5. In the Table Editor row, click on the Agent ACL column to display the ACL Selection window. Expand the folders to select the desired ACL.
6. Click **OK**. A green exclamation mark  marks the cell that has been changed and the Save to Database button becomes active.
7. Click on the Save to Database button to save your change to the ACL Manager Database.
8. Click on the Enforce button to write your changes to the device's active configuration.

---

**CAUTION:** If the ACL that you are assigning could deny contact with the device from the NetSight server, an error will occur when the device is enforced. There is an Enforce option (Allow ACLs to Deny NetSight) that turns off checking for ACLs which deny access to the device from the NetSight server. Use of this option could result in lost contact with the device. You should **not** apply an ACL that denies access to the device. If contact is denied by an ACL, you must use the device's command line interface (CLI) to remove the ACL and restore contact.

---

### Related Information

For information on related windows:

- [ACL Manager Tab](#)

For information on related tasks:

- [How to Enforce ACLs](#)

## How to Clear Threshold Alarms

---

A threshold alarm is a network alarm that is triggered when a specified value enters an unacceptable range. There are two types of threshold alarms based on the type of monitored statistics: OneView and TopN.

There are differences in how OneView and TopN threshold alarms can be cleared. This Help topic explains those differences.

For more information on creating threshold alarms, see the [How to Configure Alarms in Alarms Manager](#) and the [Edit Threshold Window](#) Help topics.

### Clearing OneView Threshold Alarms

OneView threshold alarms can be [cleared manually](#) using the Console Event Log and the Alarms tab on the Management Center [Alarms and Events tab](#). In addition, there are two ways to configure a OneView threshold alarm to clear automatically, each with different advantages:

- A OneView threshold alarm can be configured to self-clear. This is called re-arming the alarm. Re-arming allows the threshold alarm to clear itself when the monitored statistic is restored to an acceptable range, without requiring a second alarm definition. When an alarm self-clears, no action is triggered. Use a self-clearing alarm unless you want to trigger an action when the alarm clears.
- A clearing alarm can be configured to clear the OneView threshold alarm when the monitored statistic is restored to an acceptable range. Use a clearing alarm if you want to configure distinct actions for both the threshold alarm and the clearing alarm.

Here are examples of both ways to automatically clear a OneView threshold alarm.

#### Using a Self-Clearing Threshold Alarm:

##### Alarm 1

Name: High CPU

Severity: Warning

Statistic: NetSight Server CPU

Cross when value goes above 80

Re-arm when value goes below 50

## Using a Threshold Alarm and a Separate Clearing Alarm:

### Alarm 1

Name: High CPU  
Severity: Warning  
Statistic: NetSight Server CPU  
Cross when value goes above 80  
Cleared by CPU OK alarm.

### Alarm 2

Name: CPU OK  
Severity: Clear  
Statistic: NetSight Server CPU  
Cross when value goes below 50  
(No re-arm value is used.)

## Clearing Application Analytics Threshold Alarms

Application Analytics threshold alarms can be [manually cleared](#) using the Console Event Log or the Alarms tab on the Management Center [Alarms and Events tab](#).

In addition, a clearing alarm can be configured to clear the Application Analytics threshold alarm when the monitored statistic is restored to an acceptable range. Here is an example of using a threshold alarm and a separate clearing alarm:

### Alarm 1

Name: High Client Facebook Bandwidth  
Severity: Warning  
Target Type: Application/Client  
Cross when value goes above 10 megabytes  
Cleared by Client Facebook Bandwidth OK alarm.

### Alarm 2

Name: Client Facebook Bandwidth OK  
Severity: Clear  
Target Type: Application/Client  
Cross when value goes below 10 megabytes

## How to Configure Alarms in Alarms Manager

---

The Console Alarms Manager lets you configure network alarms that provide status information for a particular problem or condition on a particular network device. Alarms are triggered when certain trap or event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed.

The alarm source, which is the device, interface, or AP that is the source of the alarm event, is considered to have an alarm until the alarm is cleared. You can view alarms and alarm status in the Console Device Tree and Extreme Management Center, and also view and clear alarms in the Alarms Log in the Console Event View.

Using the [Alarms Manager window](#) (Tools > Alarm/Event > Alarms Manager), you can add a new alarm definition, which includes configuring the conditions (criteria) which will trigger the alarm, and defining the actions that will be performed to notify a person or network component about the problem, when the alarm is triggered. You can also create alarm definitions in Management Center. For more information, see [How to Configure Alarms in Extreme Management Center](#).

You can create an alarm definition that detects a problem or condition and raises an alarm, and you can also create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Link Down alarm is triggered when a device emits a linkDown trap. Then, when the device emits a linkUp trap, the Link Up alarm automatically clears the Link Down alarm.

NetSight ships with a set of default alarm definitions, which you can see listed in the Alarm Table in the Alarms Manager window. You can use these default alarms as is, or delete or modify them as desired.

This Help topic includes instructions for:

- [Defining an Alarm](#)
- [Disabling Alarms](#)
- [Viewing Alarms](#)
  - [Console](#)
  - [Extreme Management Center](#)
- [Clearing Alarms](#)







## Defining an Alarm

You can use the Alarms Manager to create new alarms and define their criteria and actions, and to edit the criteria and actions for existing alarms.


To create a new alarm or change an existing alarm:

1. From the Tools menu, select **Tools > Alarm/Event > Alarms Manager** or click the Alarms Manager icon on the toolbar. The [Alarms Manager window](#) opens.
2. **To create a new alarm:**
  - a. Click **New Alarm**. The New Alarm Name window opens.
  - b. Type a name for your new alarm and click **OK**.
  - c. Proceed to the fields below the table to configure your alarm parameters.

### To modify an existing alarm:

- a. In the Alarm Table, select the alarm that you want to change.
  - b. Proceed to the fields below the table to change your alarm parameters.
3. In the Alarm Details section, select the appropriate Alarm Severity. The alarm can have its own specified severity regardless of the severity of the event or trap that triggered it.
  -  (question mark) Set from Source - the alarm will use the severity level of the trigger event, for example a warning event.
  -  (Red) Critical - A problem with significant implications.
  -  (Orange) Error - A problem with limited implications.
  -  (Yellow) Warning - A condition that might lead to a problem.
  -  (Blue) Info - Information only; not a problem.
  -  (Green) Clear - An alarm that clears another alarm (for example, LinkUp).
4. Select the Enable Alarm checkbox to activate the alarm. You can disable an alarm to deactivate it without deleting the definition.

5. In the **Criteria** subtab, select the alarm criteria that will trigger the alarm:
  - **By Event/Trap Severity** - Triggers the alarm when a specific level of event or trap occurs. Select an event severity level (Emergency, Alert, Critical, Error, Warning, Notice, or Info) from the drop-down list. Select whether the alarm will be triggered by traps, or events, or both.
  - **By Selected Trap** - Triggers the alarm when a specific trap occurs. Click **Edit Traps** to open the [Trap Selection](#) window where you can select one or more traps that will trigger the alarm. You will be able to select from all the Trap IDs available for the devices modeled in the NetSight database.
  - **By Custom Criteria** - Define very specific criteria to trigger the alarm. Click **Edit Criteria** to open the [Edit Custom Alarm Criteria](#) window, and refer to [How to Configure Custom Alarm Criteria](#) for more information on this task.
  - **By Device Status Change** - Triggers the alarm when the operational status for a device changes: **Contact Lost** triggers the alarm when contact with a device is lost, **Contact Established** triggers the alarm when contact is restored, and **Both** will trigger the alarm when contact is lost and when contact is regained.
  - **By Threshold** - Triggers the alarm when a specified value enters an unacceptable range, for example, when CPU utilization exceeds 80% or when free disk space falls below 100 MB. Click **Edit Threshold** and then refer to the [Edit Threshold Window](#) Help topic for information on defining threshold alarms. There are two threshold alarm types: Application Analytics and OneView. This option will be disabled if your Management Center license does not include Management Center features that support threshold alarms (such as device statistics collection), and you do not have a Application Analytics license.
  - **By Flow** - Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. Click **Edit Flow Criteria** to open the [Edit Flow Criteria window](#) where you can define the flow criteria that will be used to trigger the alarm.
6. If desired, you can restrict the alarm to devices and [port elements](#) in one or more device groups. The alarm will only be raised on devices and interfaces in the selected device groups. This allows you to filter alarms to specific devices or important ports. Use the **Select Groups** button to select the desired groups.

7. In the **Actions** subtab, use the checkboxes to select the actions that will be performed when the alarm is triggered. You can test an alarm action by clicking the Test Action button . (An alarm must be saved before it can be tested.)
- **Email** - Sends an email if the alarm is triggered. Use the drop-down menu to select one of your pre-defined email lists. If no lists have been defined, the menu will be empty and you can click the **Edit Email Lists** button to define a list. (You must have your SMTP E-Mail Server options configured. Click **Set Mail Config** to open the SMTP E-Mail Server Options window where you can define your outgoing e-mail server and the sender's address for your e-mail notifications.) There are default formats for the subject and body of the email, which can be overridden by selecting the Override Content checkbox.
  - **Syslog Server** - Creates a syslog message if the alarm is triggered. Enter the IP address or hostname that identifies the syslog server where the message will be sent. There is a default format for the syslog message sent to the server, which can be overridden by selecting the Override Content checkbox.
  - **Trap Server** - Sends an SNMP trap if the alarm is triggered. Enter the IP address for a trap receiver where the trap will be sent. Valid trap receivers are systems running an SNMP Trap Service. From the Credential drop-down list select the appropriate SNMP credential that will be used when sending the trap to the trap receiver. Credentials are defined in the Profiles/Credentials tab in the Authorization/Device Access window (Tools > Authorization/Device Access). There is a default format for the trap message, which can be overridden by selecting the Override Content checkbox.
  - **isaac Service** - Sends a message to the isaac service if the alarm is triggered. The default alarm message is sent, or you can customize the message using the Override Content window. When you enable the isaac service action, it is seen as a notification in the Notifications panel in isaac. Then, when the alarm is triggered, a message is sent to isaac, and isaac forwards out the notification to alert isaac users. There is a default format for the isaac message, which can be overridden by selecting the Override Content checkbox.
  - **Program** - Runs a custom program or script on the NetSight Server if the alarm is triggered. In the Program field, enter the name of the program or use the **Select** button to open a file browser window and



choose a program. In the Working Directory field, enter the path to the directory from which the program will be executed or use the **Select** button to open a file browser window and choose a directory. Any path references within your program that are not absolute paths, will be relative to the working directory. There is a default set of arguments passed to the program, which can be overridden by selecting the Override Content checkbox.

- **Override Content** - Select this checkbox if you want to override the default content contained in the action message or action program arguments. The default content is defined in the Console Alarms options (Tools > Options > Console > Alarms). Use the **Edit Content** button to open the Edit Action Overrides window where you can override the defaults for this specific alarm action only.
8. If you want to set a limit on the number of times the alarm action will be performed for this alarm, check **Enable Action Limit** and type a number into the **Max Count** field. Once the limit is reached, the alarm is still recorded, but no further actions are performed. If you have configured multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. If Enable Action Limit is not checked, there is no limit placed on the number of times the action will be performed.
  9. You can specify a **Reset Interval** which will automatically reset the action count after the time limit specified, allowing actions to resume. If the reset interval is set to "None", then once the alarm limit is reached, the alarm will not reset unless manually reset. You can reset the action counters for all current alarms related to this alarm definition using the **Reset All** button. For example, if there is a Flow Limit Alarm on three devices, it will reset the limits on those three alarms.
  10. In the **Other Options** subtab, select the desired option for how the alarm will be cleared.
    - **No Current Alarm (Action Only)** - When this option is selected, the Alarms Manager will only perform the configured actions, but will not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source will not change, and no alarm will be added to the system.
    - **Cleared by Alarm** - This option allows you to select the alarm(s) that will be used to clear the alarm you are defining. You must first create the alarm definitions for the clearing alarms, which must have the

alarm severity set to "Clear". The clearing alarms should be triggered when the problem or condition is removed. Then, use the **Select Alarms** button to open a window where you can select one or more clearing alarms that will clear the alarm you are defining.

You can also clear alarms in the Alarms Log in the Console Event View.

11. Click **OK** to apply your settings and close the Alarms Manager window. After you add, edit, or delete an alarm definition, you must click **Apply** or **OK** for your changes to take effect.

## Disabling Alarms

There may be times when you want to disable a single alarm or all alarms. For example, you might want to temporarily disable alarms while you are performing network maintenance.

1. From the Tools menu, **select Tools > Alarm/Event > Alarms Manager**. The [Alarms Manager](#) window opens.
2. **To disable all alarms**, click the **Disable Alarms** button to the right of the Alarm table. When you disable alarms, the alarm events that trigger or clear alarms will be ignored, and no alarm actions will be performed. Click **Enable Alarms** to re-enable all alarms.
3. **To disable an individual alarm**, select the desired alarm in the Alarm table. Deselect the **Enable Alarm** checkbox in the Alarm Details section. When you disable an alarm, the alarm events that trigger the alarm will be ignored, and no alarm actions will be performed.

## Viewing Alarms

You can view device/alarm status in multiple places throughout Console and Management Center.

### *Console*

The Console Status Bar displays a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) that is present in the entire system. If there are no current alarms, the status will read all zeroes. Click on an indicator to view details on the alarms with that severity.

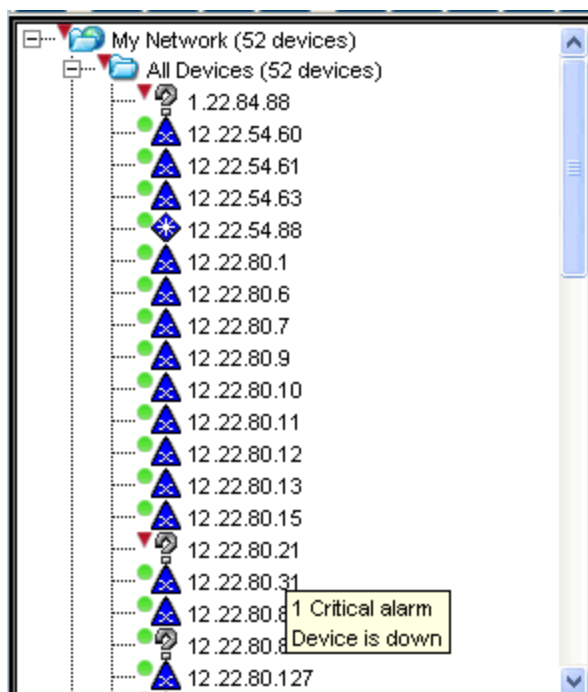


## Console Device Tree

In Console, the device tree displays an integrated alarm/device status that rolls up into each device group. The colored circle next to the device or group icon indicates device status as well as the severity of the most severe alarm on the device or in the device group.

- ▼ (Red) Critical - There is a critical alarm and the device is down, or some of the devices in the group are down.
- ► (Orange) Error - There is a problem with limited implications on the device or a device in the group.
- ▲ (Yellow) Warning - There is a condition that might lead to a problem on the device or a device in the group.
- ■ (Blue) Info - There is an information only alarm on the device or a device in the group.
- ● (Green) Clear - There are no alarms and the device is up, or all the devices in the group are up.

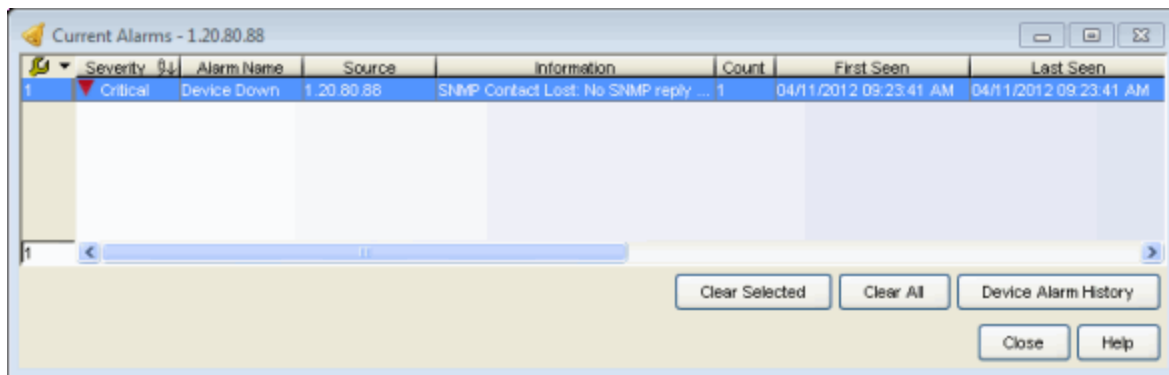
Hover over the device to see a tooltip with the alarm/device status.



## Console Device Current Alarms

Right-click on a device or device group in the Console device tree and select View Current Alarms to open a window that displays current alarm information for the device or device group.

- Use the **Clear Selected** or **Clear All** buttons in the window to clear selected alarms or clear all alarms for the device or device group.
- Use the **Device Alarm History** button to view information about all current and past alarms for the device or device group.
- Right-click on an alarm to view an [alarm history](#) for that specific alarm.
- Right-click on an alarm to view the [alarm limits](#) and action counters configured for that alarm.



You can also right-click on a device or device group in the Console device tree and select Clear Current Alarms to clear the current alarms for the device or device group.

## Console Alarms Event View

Select the Alarms tab in the Console Event View to view information about current network alarms.

- Use the **Clear Selected** or **Clear All** buttons on the tab to clear selected alarms or clear all alarms.
- Use the **All Alarm History** button to view information about all current and past alarms.
- Right-click on an alarm to view an [alarm history](#) for that specific alarm.
- Right-click on an alarm to view the [alarm limits](#) and action counters configured for that alarm.

Severity	Alarm Name	Source	Information	Count	First Seen	Last Seen
1 Critical	Device Down	1.23.85.88	SNMP Contact Lost: No SNMP reply fro...	1	04/11/2012 08:23:41 AM	04/11/2012 08:23:41 AM
2 Critical	Device Down	12122160.21	SNMP Contact Lost: No SNMP reply fro...	1	04/12/2012 08:13:07 AM	04/12/2012 08:13:07 AM
3 Critical	Device Down	12122165.3	SNMP Contact Lost: No SNMP reply fro...	1	04/12/2012 08:13:09 AM	04/12/2012 08:13:09 AM
4 Critical	Device Down	12122168.169	SNMP Contact Lost: No SNMP reply fro...	1	04/12/2012 08:13:10 AM	04/12/2012 08:13:10 AM

4

Clear Selected Clear All All Alarm History

Console Alarms Traps Syslog Automated Security Inventory Policy Control Console Policy NAC

0%

### Extreme Management Center

Every Management Center page includes a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) that is present in the entire system. If there are no current alarms, the status displays all zeroes. Click on an indicator to view details on the alarms with that severity.



### Extreme Management Center Alarms and Events Tab

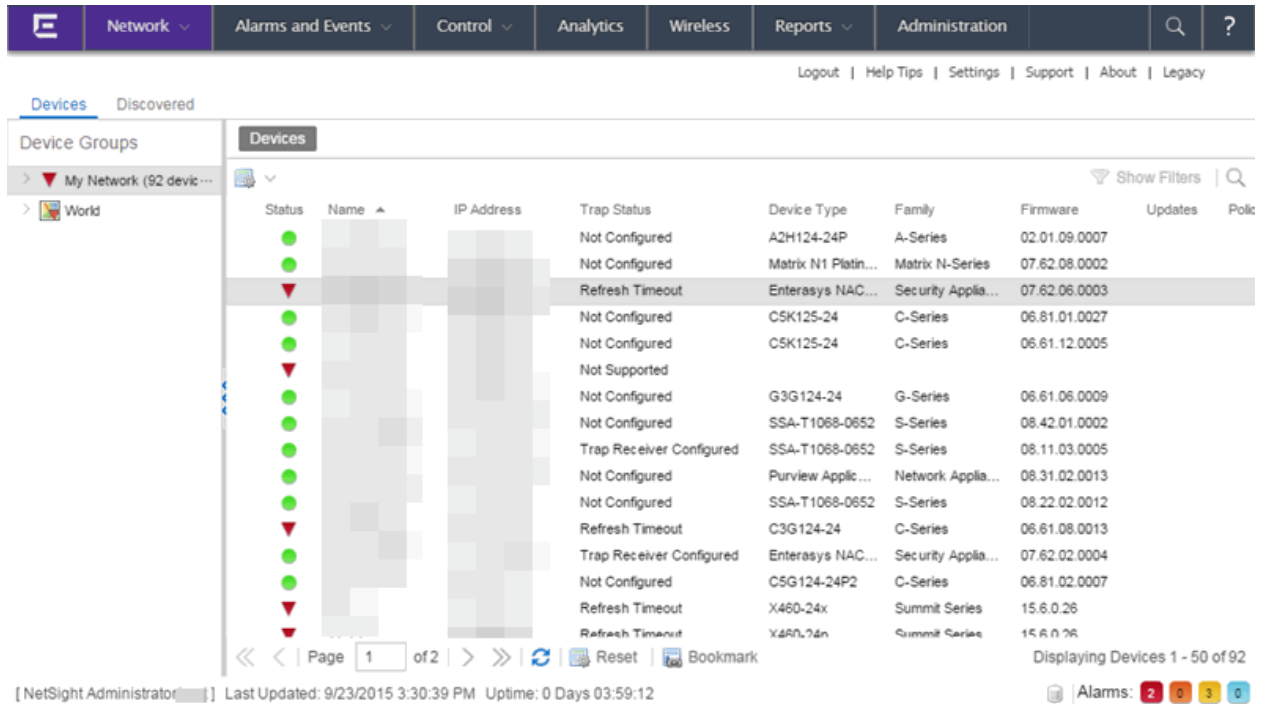
You can view current alarm information in the Alarms view under the Management Center [Alarms and Events tab](#). Use the configuration menu button or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason that the alarm was cleared, which is recorded in the Alarm History.

The screenshot shows the 'Alarms' tab in the Alarms Manager. The interface includes a navigation bar with tabs for Network, Alarms and Events, Control, Analytics, Wireless, Reports, and Administration. Below the navigation bar, there are links for Logout, Settings, Support, About, and Legacy. The main content area displays a table of alarms with columns for Severity, Last Seen, Seen, Source, Alarm Name, Information, and First Seen. The table contains five rows of alarm data, including 'Purview Appliance Do...', 'Host Memory % Usage', 'Device Down', and 'Controller Failed SSH...'. At the bottom of the page, there is a pagination control showing 'Page 1 of 1' and a status bar indicating 'Displaying Alarms 1 - 5 of 5' and 'Alarms: 2 0 3 0'.

Severity	Last Seen	Seen	Source	Alarm Name	Information	First Seen
▼	9/24/2015 1:29:34 PM	12		Purview Appliance Do...	Contact lost with Purview Appliance [redacted] amqp'	9/24/2015 10:21:34 ...
▲	9/23/2015 5:48:12 PM	1		Host Memory % Usage	statistic: DeviceHrPhysicalMemoryUsed, value: [redacted] ..	9/23/2015 5:48:12 PM
▼	9/23/2015 5:07:25 PM	1		Device Down	SNMP Contact Lost: No SNMP reply from device [redacted] ..	9/23/2015 5:07:25 PM
▲	9/23/2015 12:01:36 ...	2		Controller Failed SSH...	Failed to establish SSH c onnection with controller [redacted] ..	9/23/2015 11:31:54 ...
▲	9/23/2015 12:01:36 ...	2		Controller Failed SSH...	Failed to establish SSH c onnection with controller [redacted] ..	9/23/2015 11:31:55 ...

## Extreme Management Center Network Tab

You can view alarm/device status in the Status column on the **Network** tab. The colored circle indicates the severity of the most severe alarm on the device, and the number indicates how many alarms of that severity are present. A green icon indicates that there are no alarms and the device is up. A red icon indicates a critical alarm or the device is down. Click on the alarm/device status icon to open a new page with detailed information about the alarms for that device.



## Clearing Alarms

An alarm can be cleared manually or automatically.

To clear an alarm manually:

- In the **Alarms** tab in the Console Event View, use the **Clear Selected** or **Clear All** buttons to clear a selected alarm or clear all alarms.
- In the **Alarms** tab on the Management Center [Alarms and Events](#) tab, use the configuration menu button or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason that the alarm was cleared, which is recorded in the [Alarm History](#).

To clear an alarm automatically:

An alarm is cleared automatically by another alarm called a "Clearing Alarm". For example, a Link Up alarm can be created so that when a device emits a linkUp trap, the alarm will automatically clear a Link Down alarm.

Clearing Alarms are configured in the [Alarms Manager window](#) with an Alarm Severity set to Clear. The alarm is then defined so that when it is triggered, it removes an alarm rather than adds one.

In addition, a OneView threshold alarm can be configured to "self-clear" (see [How to Clear Threshold Alarms](#) for more information). This is called re-arming the alarm. Re-arming allows the threshold alarm to clear itself when the monitored statistic is restored to an acceptable range, without requiring a clearing alarm. When an alarm self-clears, no action is triggered.

---

## Related Information

For information on related windows:

- [Alarms Manager Window](#)
- [Edit Custom Alarm Criteria Window](#)
- [Trap Selection Window](#)

For information on related tasks:

- [How to Configure Custom Alarm Criteria](#)
- [How to Configure Alarms in Extreme Management Center](#)



## How to Configure Custom Alarm Criteria

---

The Console Alarms Manager lets you configure network alarms that provide status information for problems on your network. Alarms are triggered when certain trap or event conditions occur on your network. Alarms Manager lets you define very specific criteria to trigger an alarm using the [Edit Custom Alarm Criteria window](#).

To define custom alarm criteria:

1. In the [Alarms Manager window](#), select **By Custom Criteria** (in the Criteria subtab) and click **Edit Criteria** to open the Edit Custom Alarm Criteria window.
2. In the window, each option lets you select one or more attributes to match against in the trap or event, in order to trigger the alarm. For each option, if you check the **Match On** box, then Alarms Manager filters based on that category. If you don't check the **Match On** box, then Alarms Manager doesn't filter based on that category, and as a result, matches everything for that category. However, if you don't check any **Match On** boxes, then Alarms Manager won't match any trap or event.

Check the **Match On** checkboxes that you want to define for this alarm and select attributes within each category to be matched.

### Match on Severity

Select one or more severity levels to match against.

- **Match Selected** - The reported Severity is matched against any of the Severity levels selected in the list.
- **Exclude Selected** - The reported Severity matches if it is not one of the Severity levels selected in the list.

### Match on Category

Select one or more event categories to match against the Category column of the event. An event category is a way to group related events. For example, all events related to device discovery would be in the "Discover" category.

- **Match Selected** - The reported Category is matched against any of the categories selected in the list.

- **Exclude Selected** - The reported Category matches if it is not one of the categories selected in the list.

#### Match on Type

Select one or more message types (Event, Inform, Trap) to match against the Type column of the event.

- **Match Selected** - The reported Type is matched against any of the types selected in the list.
- **Exclude Selected** - The reported Type matches if it is not one of the message types selected in the list.

#### Match on Event

Select one or more event types to match against the Event column of the event.

- **Match Selected** - The reported Event is matched against any of the event types selected in the list.
- **Exclude Selected** - The reported Event matches if it is not one of the event types selected in the list.

#### Match on Host or IP/Subnet

Select one or more host names or IP/Subnet addresses to match against the value of the address appearing in the Source column of the event. The list of host names and IP/ Subnet addresses can be edited by clicking the **Edit List** button to open the [Match Host window](#).

- **Match Selected** - The reported host name or IP/Subnet address is matched against any of the host or IP/Subnets selected in the list.
- **Exclude Selected** - The reported host name or IP/Subnet address matches if it is not one of the host or IP/Subnets selected in the list.

#### Match on Log Manager

Select one or more Event Logs to match against.

- **Match Selected** - The log where the event was received is matched against any of the logs selected in the list.
- **Exclude Selected** - The log where the event was received matches if it is not one of the logs selected in the list.

### Match on Information Text

Select one or more text strings (phrases) to match against text in the Information column of the event or trap. The list of text phrases can be edited by clicking the **Edit List** button to open the [Match Phrase List window](#).

- **Match Selected** - The Information text string is matched against one or more phrase selected from the list.
- **Exclude Selected** - The information text string matches if it is not one of the phrases selected from the list.

3. When satisfied with your selections, click **OK** to close the window.

---

### Related Information

For information on related windows:

- [Edit Custom Alarm Criteria Window](#)
- [Alarms Manager Window](#)
- [Match Host IP or Subnet List](#)
- [Match Phrase List](#)

For information on related tasks:

- [How to Configure Alarms](#)

## How to Configure the SNMP Trap Service

---

The NetSight SNMP Trap Service (snmptrapd) receives SNMP *trap* and *inform* messages from your network devices and logs them into the Event Log. SNMPv1/v2 traps are sent by devices using a community name, and are accepted by the Trap Service regardless of what the community name is. For SNMPv3 traps and informs, the Trap Service must know the credentials (user name/passwords) and the SNMP Engine ID (required for traps) of the sending agent on the device before a trap or inform can be received. This information is configured in the snmptrapd.conf file. If this information is not configured, trap and inform messages will be dropped by the Trap Service. For more information, see [Traps and Informs](#).

Use the [Trap Receiver Configuration](#) window to configure the information needed to receive trap information from the devices on your network. The window lets you create a list of IP addresses of the systems that will receive traps (trap receiver addresses). It also lets you configure the snmptrapd.conf file with the credentials and Engine IDs required for your SNMPv3 devices.

Instructions on:

- [Configuring Trap Receivers](#)
- [Configuring the snmptrapd.conf File](#)
- [Restarting the SNMP Trap Service](#)

### Configuring Trap Receivers

Use these steps to create a list of trap receiver addresses. These are the addresses of the systems that will receive trap information from your network devices.

1. In Console's left-panel tree, right-click on one or more devices or device groups, and select **Trap Receiver Configuration**. The [Trap Receiver Configuration](#) window opens.
2. In the **Configuration** tab, the table at the bottom lists the selected devices and their current trap receiver information.
3. In the top table, create a list of trap receiver addresses to set on the devices. When the Trap Receiver Configuration window is initially opened, this table lists the Console workstation as the only trap receiver. Click the **Update**

**From All/Selected Devices** button to update the table with the current trap receiver information from the selected devices. You can also manually add trap receivers to the table, using the right-click menu, tab key, and arrow keys. Tab through the table columns and modify each entry as desired:

- a. Check the **Configure** checkbox if you want this particular trap receiver entry to be set on the selected devices when you **Apply** your trap receiver configuration settings.
  - b. Use the **Priority** column to specify the order in which trap receiver entries will be set on the selected devices, with the lowest number having the highest priority. When you **Apply** your trap receiver settings, Console writes the Trap Receiver IPs to each device in order, starting with the highest priority (the lowest number) until all are written or a device cannot accept any more.
  - c. Enter the **Trap Receiver IP** address for a trap receiver (the system where devices will send traps). Trap receivers systems must be running an SNMP Trap Service.
  - d. Select the supported message **type**: Trap, Inform, or Both.
  - e. Use the drop-down list to select the **Trap Credential** for the trap receiver. Note that when a credential appears within angle brackets (< *credential name*>), it indicates that the community or user name could not be found among the credentials created in Console. When this happens, a temporary credential name is created, derived from the community or user name on the device.
4. If desired, select the checkbox to **remove or update existing trap receiver IPs on devices during Apply operation**. When checked, an Apply operation will update the Trap Configuration table on the devices to match the enabled entries in this table, by adding, modifying, and removing entries as necessary. Entries on the device that were created via CLI are never deleted or modified. When unchecked, an Apply operation will add entries from this table to the devices Trap Configuration table. Existing entries on the devices are not modified in any way and no duplicate addresses are created.
  5. In the Trap Receivers on Devices table, select the devices that you want to apply the configuration to. If no devices are selected, then all devices in the table will be updated. Click **Apply to All/Selected Devices** to write (set) the trap receiver IPs listed in the Trap Receiver Configuration table to the selected devices.

## Configuring the snmptrapd.conf File

Use these steps to configure the snmptrapd.conf file with the credential and Engine ID information required for SNMPv3 devices.

1. In Console's left-panel tree, right-click on one or more devices or device groups, and select **Trap Receiver Configuration**. The [Trap Receiver Configuration](#) window opens.
2. Click the **snmptrapd** tab. The Credential Table is displayed listing the credential information for the selected devices.
3. The **Credential Name** column can be edited by clicking on the column to display a drop-down list that contains all SNMPv3 credentials from the NetSight database. (Go to the Authorization/Device Access - Profiles/Credentials tab to create a credential, if necessary.) Once an edit is made, an asterisk is displayed in the **Modified** column to show which rows were changed.
4. You can also add new entries to the table. Click **Add Entry** to add a new row to the table. The Credential Name column will display the ReadOnly credential for the default Profile. The Engine ID and Credential Name columns can be configured for new rows. An Engine ID is only necessary for devices sending trap messages; it is not necessary for informs.
5. Select the rows you want to add to the snmptrapd.conf file, and click **Add Entry**.

- NOTES:**
1. You can also add entries to the configuration file by typing user credentials directly into the snmptrapd.conf Text area. Refer to the information in the Text area for instructions and examples.
  2. To modify an entry you have added to the file, you must first remove the entry from the file and then add a new entry via the table. To remove entries from the snmptrapd.conf file, you must select the entry in the Text area, and press Delete.


6. Click **Save** and **Close**. The user credentials have been added to the snmptrapd.conf file.
7. After making changes, you must restart the SNMP Trap Service on the NetSight Server. Refer to [Restarting the SNMP Trap Service](#) for more information.

- 
- NOTES:**
1. You can manually add user information directly to the `snmptrapd.conf` file using a text editor. Instructions are provided in the `snmptrapd.conf` file located on the server in the `<install directory>\NetSight\appdata` directory.
  2. The `snmptrapd.conf` file is not preserved during the Console Uninstall.
- 

## Restarting the SNMP Trap Service


Depending on the system where the NetSight Server is running, there are several ways to restart the SNMP Trap service.

*Restarting the service locally on the NetSight Server host system:*

Windows	Linux
<p>Using the Services Manager:</p> <ol style="list-style-type: none"> <li>Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar).</li> <li>Locate the Services Manager icon (  ) and right-click it.</li> <li>Select <b>SNMPTrap</b> &gt; <b>Restart</b>.</li> </ol> <p>Using Windows Services:</p> <ol style="list-style-type: none"> <li>From the Control Panel, access the Administrative Tools &gt; Services window.</li> <li>Locate the <code>snmptrapd</code> service and select "Restart the service."</li> </ol>	<ol style="list-style-type: none"> <li>Navigate to the <code>etc/init.d</code> directory.</li> <li>Type the command: <code>nssnmptrapd stop</code></li> <li>Press <b>Enter</b>.</li> <li>Type the command: <code>nssnmptrapd start</code></li> <li>Press <b>Enter</b>.</li> </ol>

---

*Restarting the service remotely from a NetSight Client host system:*

Windows	Linux
<p>Restarting the service remotely on Windows host systems is only possible if both the Client and Server are capable of running <b>Remote Desktop</b> (a feature of Windows XP Professional) or through the use of a third-party facility that provides similar capabilities to Remote Desktop.</p> <p>When you can access the Services Manager on the remote system using either Remote Desktop or a third-party program, you can restart the service as follows:</p> <ol style="list-style-type: none"> <li>Go to the Taskbar Notification Area of the remote desktop.</li> <li>Locate the Services Manager and right click the icon (  ).</li> <li>Select <b>SNMPTrap</b> &gt; <b>Restart</b>.</li> </ol>	<ol style="list-style-type: none"> <li>Telnet to the server and login as an administrative user.</li> <li>Navigate to the <code>etc/init.d</code> directory.</li> <li>Type the command: <code>nssnmptrapd stop</code></li> <li>Press <b>Enter</b>.</li> <li>Type the command: <code>nssnmptrapd start</code></li> <li>Press <b>Enter</b>.</li> <li>Log out and close the telnet session.</li> </ol>

## Related Information

For information on related windows:

- [Trap Receiver Configuration Window](#)
- Authorization/Device Access Window - Profiles/Credentials Tab

For information on related concepts:

- [Traps and Informs](#)



## How to Create ACL Rules

---

Traffic that arrives at a router port is either accepted or blocked according to the rules contained in an Access Control List (ACL). Rules **Permit** or **Deny** traffic that matches criteria defined by its parameters. A rule's parameters can define a specific source/destination or be set to Any, which creates an automatic match for the source/destination. Rules can apply to one or more protocols. The ACL is examined from top to bottom, with the first rule that matches the packet determining the fate of that packet (dropped or forwarded). If there are no matching rules, the packet is denied. To change this behavior, add a rule that permits everything as the last rule in the ACL.


Individual rules within an ACL can be disabled by commenting the rule. Commenting suppresses enforcement of a rule. When a rule is commented, it appears as a gray icon in the ACL Editor.

Instructions on:

- [Creating a Rule](#)
- [Modifying a Rule](#)
- [Commenting and Uncommenting a Rule](#)
- [Deleting a Rule](#)


### Creating a Rule

ACL rules are created using the ACL Editor.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, select the ACL where you would like to create the rule.
3. In the right-panel Editor tab, click the **New** button.
4. The Add to ACL window opens where you can create the new rule. The parameters/fields in this window will change according to the rule type selected. Refer to the [Add to ACL](#) help topic for information on the specific fields.
5. Click **OK**. The window closes and the rule appears in the left-panel tree.


## Modifying a Rule

You can modify a rule's parameters using the ACL Editor.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, select the rule that you would like to modify.
3. In the right-panel Editor tab, click the **Edit** button.
4. The Edit ACL window opens where you can modify the rule. The parameters/fields in this window will change according to the rule type selected. Refer to the [Add to ACL](#) help topic for information on the specific fields.
5. Click **OK**.


## Commenting and Uncommenting a Rule

Rules can be disabled or enabled by commenting or uncommenting, respectively, the line in the ACL that defines the rule.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, select the rule that you would like to comment out or uncomment.
3. Right-click on the rule and select Comment Out (disable) or Uncomment (enable).

## Deleting a Rule

You can delete a rule using the ACL Editor.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, select the rule that you would like to delete.
3. Right-click on the rule and select Delete. The rule is deleted from the left-panel tree.

---

## Related Information

For information on related windows:

- [ACL Editor](#)
- [Add to ACL Window](#)

## How to Discover Devices

---

The Discover tool allows you to discover the physical elements (devices) of your network, and add them to the NetSight database. You can perform a discover on a specified range of IP addresses, or perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices. Discover automatically explores the defined network segment and creates a list of discovered devices. You can then save the discovered devices to the NetSight database where they are displayed in the left-panel tree in the Console main window.

The Discover window provides two kinds of discover operations:

- [IP Range Discover](#) -- performs a discover based on one or more IP address ranges. An IP Range Discover discovers all devices within the specified IP address range(s).
- [CDP Seed IP Discover](#) -- performs discover operations of CDP-compliant devices in the network, starting with a one or more CDP seed devices.

Deciding what type of discover to use depends on your specific network configuration. Generally, if your network has all CDP-compliant devices that are configured with the same SNMP access parameters, the CDP Seed IP Discover is recommended. If your network has no CDP-compliant devices, or a mix of CDP and non-CDP-compliant devices, the IP Range Discover is recommended.

---

**TIP:** To discover a network with both CDP-compliant and non-CDP-compliant devices, you can either perform an IP Range Discover, or perform a CDP Seed IP Discover to first discover all the CDP-compliant devices, and then perform an IP Range discover or use Add Device to add the non-CDP-compliant devices.

---

You can specify Discover options using the [Discover view](#) of the Options window (**Tools > Options**). Discover options include setting the timeout value (how long Discover waits before re-trying to contact a device), and the number of IP addresses Discover will try to contact simultaneously.

There may be an occasion when you want to add a device to the NetSight database without using a discover process. For example, you may want to monitor and manage one specific device for testing purposes. In that case, you would add a device using the [Add Device Window](#).

## Configuring Ping for Linux and Mac OS X Clients

The first time you run a **Ping Only Discover** from a Mac OS X or Linux client, the Discover will fail because jping is not executable. To fix this problem, perform the following steps to give the jping executable root privileges, allowing it to open up a socket for communication back to a NetSight client.

### On a Linux client (32-bit or 64-bit):


1. Open an xterm where you are logged in as root.
2. `mkdir -p /var/Extreme_Networks/NetSight`
3. `cp ~/NetSight/System/<.bin32 or .bin64>/jping /var/Extreme_Networks/NetSight`
4. `chmod a+x /var/Extreme_Networks/NetSight/jping`
5. `chmod u+s /var/Extreme_Networks/NetSight/jping`

### On a Mac OS X client (64-bit):

1. Open a terminal window.
2. `cd ~/NetSight/System/.bin64`
3. `sudo chown root jping`

## IP Range Discover

Use the IP Range Discover to perform a discover based on one or more IP address ranges. The results of the discover process are displayed in the [Discover Results table](#). You can then save the discovered devices to the NetSight database where they are displayed in the left-panel tree.

1. Select **Tools > Discover** from the menu bar or click the Discover button  in the toolbar. The Discover window opens.
2. Select the **IP Range tab**.
3. At the top of the tab is a table where you specify the IP address ranges. Each row defines a single range. When you first open the tab, a default range is displayed based on the IP address of the Console workstation.

---

**NOTE:** Use Console's table options and tools to filter, find, sort, print, and export information in the table, and to customize table settings. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

---

4. To add a new range, right-click on an existing row and select **Insert Row**. A new row will be created above the selected row using the same parameters. (Using your keyboard's down arrow or tabbing past the last row will also create a new row.) The position of a row determines the range's **Precedence**, as indicated in the second column. Precedence determines which parameters will be used if a device is in more than one range (the lower number yields higher precedence). For example, if a device is in two ranges -- one range with a precedence of 1 using an SNMPv3 profile, and one range with a precedence of 2 using an SNMPv1 profile -- the device will be saved with the SNMPv3 profile because that range has the higher precedence.
5. To edit a range, simply tab through the parameters and either enter a new value or use the drop-down list to select a value.
  - **Enabled** -- Select the checkbox to enable Discover for this IP address range. Only enabled ranges are searched when a discover operation is performed.
  - **Start IP** -- Enter the IP address at which the range should begin.
  - **End IP** -- Enter the IP address at which the range should end.
  - **Profile** -- Use the drop-down list to select the access Profile that will give the Discover tool read access to the devices you want to discover. **Ping Only** allows discovering devices such as workstations and other devices that are not configured for SNMP. If Ping Only is selected, the Poll Type must be set to **Ping**. (See the [Configuring Ping for Linux and Mac OS X Clients](#) section above.) Click the **Profile Details** button to open the Authorization/Device Access Window - Profiles/Credentials Tab where you can create and edit Console profiles. If you discover an existing device using a different profile than the device is already using in the database, saving the device will overwrite the profile currently being used in the database.
  - **Context** -- SNMP Context lets you specify a context that has been configured on a device. The context lets you access a subset of MIB objects related to that context. Console lets you specify a SNMP Context for both SNMPv1/v2 and SNMPv3.

The use of context differs depending on the protocol version being used with the credentials used by the selected **Profile**:

- When used, with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.
- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, a SNMPv1 or SNMPv2 credential (community name) can be mapped, through Local Management, to a particular SNMP context on the device. Thus, when SNMPv1/v2 credentials are used with a Context entry, access is granted to the subset of MIB objects associated with that context. If the credential used is accepted, but the context specified doesn't match a context configured on the device, access is granted to the default context.

Console treats each context for a given device (IP address) as a distinct device. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to your device *Configuration Guide* for more information about setting and showing SNMP contexts.

- **Poll Type** -- Use the drop-down list to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. If you discover an existing device using a different poll type than the device is already using in the database, saving the device will overwrite the poll type currently being used in the database.

---

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

---

- **Poll Group** -- Use the drop-down list to select a Poll Group for the discovered devices. Console provides three distinct poll groups (defined in the Status Polling view of the Suite-Wide Options window) that each specify a unique poll frequency. When you save newly discovered devices to the database, they will be polled with the

poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

---

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

---

- **Vendor** -- Use the drop-down list to specify whether you want to discover all devices or only Extreme devices.
6. Click **Discover** to begin the discover operation. Discovered devices are listed in the [Discover Results table](#). The progress of each range discover is displayed as a percentage in the corresponding Progress column.
- 

**NOTE:** When a Discover operation is initiated, all rows that are enabled are checked for validity. If any rows have invalid parameters, the Progress column for that row will alert you to the invalid entry.

---

7. After the discover is complete you can save all or selected devices to the database:
- Click **Save All** to save all the discovered devices to the NetSight database.
  - Use the **Hide Duplicate and Empty MACs** checkbox to filter the Discover Results table to show one discovered device per MAC address. (When routed interfaces cause the same device to be discovered multiple times, this checkbox filters out duplicate entries.) Click **Save** to save the filtered devices to the database.
  - Select only the desired devices in the Discovered Devices table and click **Save** to save those devices to the database.
  - Select all or some of the devices and right click one of the selected devices and select **Add Devices to Group** to open a window where you can select a specific group where the devices will be saved.

To remove a device from the table, select the device and click **Remove**.

---

**NOTE:** If the IP Range includes broadcast addresses (.0, .255, .127, .128, depending on the subnet mask), the addresses may be discovered as devices. To make the polling of devices in the Console tree as efficient as possible, these addresses should be removed and not saved to the database.

---

It is recommended that you backup the NetSight database (**Tools > Server Information > Database Tab**) after you have saved your discovered devices.



8. To delete an IP range, right-click on the table row and select Delete Row. You can select and delete multiple rows.


---

**TIP:** Specify as narrow an IP address range as possible. The wider the range, the longer it will take to perform the discover. For example, if you are discovering IP addresses 111.111.111.20 through 30, and 111.111.111.240 through 250, it is faster to create two separate discovers for each range rather than performing one discover for 111.111.111.20 through 250.

---

## CDP Seed IP Discover

Use the [Discover window](#) to perform a discover for CDP-compliant devices in the network. The results of the discover process are displayed in the [Discover Results table](#). You can then save the discovered devices to the NetSight database where they are displayed in the left-panel tree.

1. Select **Tools > Discover** in the menu bar or click the Discover button  in the toolbar. The Discover window opens.
2. Select the **CDP Seed IP** tab. You can define multiple CDP Seed discover operations in the view. Define each discover operation in a separate row. To add a new range, right-click on an existing row and select **Insert Row**. A new row will be created above the selected row using the same parameters. (Using your keyboard's down arrow or tabbing past the last row will also create a new row.) The position of a row determines the **Precedence**, as indicated in the second column. Precedence determines which parameters will be used if a device can be discovered by the parameters in than one row (the lower number yields higher precedence). For example, if a device could be discovered by two discover operations -- one with a precedence of 1 using an SNMPv3 profile, and the other with a precedence of 2 using an SNMPv1 profile -- the device will be saved with the SNMPv3 profile because that range has the higher precedence.
3. To edit a row, simply tab through the parameters and either enter a new value or use the drop-down list to select a value.
4. In the **Seed IP** column, enter the IP address for your CDP seed device. Discover will use the seed device's CDP Neighbor Table to begin discovering all CDP-compliant devices.
5. Use the drop-down list in the Profile column to select the access Profile that will give the Discover tool read access to the devices you wish to discover.

Click the **Profile Details** button to open the Authorization/Device Access Window - Profiles/Credentials Tab where you can create and edit Console profiles. If you discover an existing device using a different profile than the device is already using in the database, saving the device will overwrite the profile currently being used in the database.

6. Use the drop-down list to select the **Poll Type** used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. (See the [note above](#) about Ping Only Discovers.) If you discover an existing device using a different poll type than the device is already using in the database, saving the device will overwrite the poll type currently being used in the database.

---

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

---

7. Use the drop-down list to select a **Poll Group** for the discovered devices. Console provides three distinct poll groups (defined in the Status Polling view of the Suite-Wide Options window) that each specify a unique poll frequency. When you save newly discovered devices to the database, they will be polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

---

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

---

8. Click **Discover**. Discovered devices are listed in the [Discover Results table](#).

---

**NOTE:** If CDP is not enabled on a seed device, a message is displayed, asking if you would like to enable CDP. **Yes** enables CDP in the device, waits for 30 seconds, then continues with the discovery. **No** cancels discovery using that seed device.

---

9. After the discover is complete you can save all or selected devices to the database:
  - Click **Save All** to save all the discovered devices to the NetSight database.
  - Use the **Hide Duplicate and Empty MACs** checkbox to filter the Discover Results table to show one discovered device per MAC address. (When routed interfaces cause the same device to be

discovered multiple times, this checkbox filters out duplicate entries.) Click **Save** to save the filtered devices to the database.

- Select only the desired devices in the Discovered Devices table and click **Save** to save those devices to the database.
- Select all or some of the devices and right click one of the selected devices and select **Add Devices to a Group** to open a window where you can select a specific group where the devices will be saved.

To remove a device from the table, select the device and click **Remove**.

---

**NOTE:** It is recommended that you backup the NetSight database (**Tools > Server Information > Database Tab**) after you have saved your discovered devices.

---

## Related Information

For information on related windows:

- [Discover Window](#)

For information on related tasks:

- [Setting Discover Options](#)

## How to Download Firmware

---

You can download a firmware image file to a device using the [Firmware Image Download window](#). You must have a TFTP server running to perform the download operation.

---

**NOTES:** Console does not support firmware download for the RoamAbout R2.

This window is only available on devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

---

1. From the main Console window, right-click the device in the left panel and select **Firmware Image Download** from the menu. The Firmware Image Download window opens. (To open the window in Device Manager, select **Utilities > Firmware Image Download** from the Device View menu bar.)
2. In the Operations area, select the desired type of operation:
  - **Download** -- Performs a download of the specified firmware image to the device. This operation will not activate the new firmware. A Reset operation must be performed to activate the downloaded image.
  - **Download & Reset** -- Performs a download of the specified firmware image to the device and resets the device with the new image as soon as the download is complete.
  - **Reset** -- Resets the device so that new firmware can be activated.
3. In the **Download Settings** area, specify the TFTP server to perform the download operation. You can enter the TFTP server's IP address, or use the dropdown list to select the TFTP server to perform the download operation. This list contains up to seven IP addresses: the IP address for the local workstation (local), the IP address of the TFTP server last set on the device (current), and up to five previously entered IP addresses. Greater than five addresses can be entered during a particular TFTP Download session, but only five are retained after this window is closed.
4. If your TFTP server is configured with a root directory, select the **Server uses Root Path** checkbox, and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to download files from this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox

will be selected with the root path as specified in the Services for NetSight Server view of the Suite-Wide Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

5. In the **Full Image Path Field**, enter the full path and filename of the image file you want to download to the device. You can also use the dropdown list to select a path and filename or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a Root Path, the browse capability is limited to the directories below that root path.
- 

**NOTE:** The **Path to Set on Device** field displays the target path and filename as it will be set on the device. If the Server Uses Root Path checkbox is selected, the specified root path is stripped from the full path and filename. If the checkbox is not selected, this field displays the same path as the Full Image Path field.

---

6. Click **Apply** to initiate the download operation. For an explanation of status messages, see the [Firmware Image Download Window](#) Help topic.
  7. If you have performed a Download operation (versus a Download & Reset operation), you must perform a Reset operation to activate the new firmware.
    - a. In the **Operation** area, select the Reset option.
    - b. Click **Apply** to reset the device and activate the new firmware.
- 

## Related Information

For information on related windows:

- [Firmware Image Download Window](#)

For information on related tasks:

- [How to Save and Restore Configuration Files](#)

## How to Enforce ACLs

---


After ACLs are assigned to interfaces or agent services in ACL Manager, they can be written to the device's active configuration using the Enforce operation. It is important to understand that using ACL Manager to manage and assign ACLs does not change the ACLs on the device until the Enforce operation is used. In ACL Manager you are managing a "view" of your ACL data that is stored in the NetSight database. You then use the Enforce operation to write that data to the device's active configuration.

ACL Manager is configured by default to delete unused ACLs from a device when ACLs are enforced. You can change this behavior by deselecting the Enforce option "Delete Unused ACLs." Refer to ACL Manager Enforce options for more information.

## How ACL Names are Determined on a Device

It is important to understand how ACL Manager allocates a new name for an ACL on a device. If you create a new ACL named "new\_acl" and assign it to an interface on a device, when you enforce, ACL Manager determines that ACL "new\_acl" needs to be copied to the device. If the device only supports numbered ACLs, then "new\_acl" would be an invalid name and ACL Manager must assign a new name for the ACL on that device. If the ACL is an extended ACL, then only ACL 100-199 can be used. So, ACL Manager considers using 100. If 100 is already in use, ACL Manager will consider 101. If 101 is excluded (via the Exclude ACL Range option) then ACL Manager will consider 102, 103, 104 and so on, until it finds a number that is not used and not excluded.

To enforce ACLs:

1. In the Console left-panel tree, select the device, devices, or Device Group that you wish to enforce. Click on the ACL Manager right-panel tab.
2. Click on the Enforce button . A last-chance message appears before the action is performed. Click **Yes** to enforce ACLs.

If errors are encountered during the Enforce operation, a message appears indicating an error and details are available from the Event Log. When the enforce action is successful, no messages appear. However, the successful operation is recorded in the Event Log and displayed on the Status Bar.

## Related Information

For information on related windows:

- [ACL Verification Results Window](#)
- [ACL Manager Options Window](#)

For information on related tasks:

- [How to Assign ACLs](#)
- [How to Verify ACLs](#)

## How to Export and Import a Device List

---

You can export a device list from NetSight Console to a text file that lists all the devices that are members of one or more selected device groups. The file is created as a .ngf file (NetSight Generated Format), which is compatible with other NetSight applications where it can be imported. Likewise, device lists that are exported from other NetSight applications, or files that are manually created in a compatible format, can be imported into the NetSight database. You can also export a database backup file from Ridgeline that you can import into NetSight Console.

### Import-Export File Format

The device list import-export file from NetSight Console is a text file (ASCII) with each line describing a specific device, using **NetSight Generated Format** (NGF), while the import-export file from Ridgeline is saved as a .sql file by default. The information for each device must be on a separate line with no line breaks in the string. Devices are identified by an IP address (the only mandatory attribute) and a set of optional attributes that define access parameters. When devices are exported, Console defaults to a .ngf file extension and Ridgeline defaults to a .sql file extension. However, these can be changed or omitted, without affecting the import or export operation.

SNMPv1/v2 devices and SNMPv3 devices use different NetSight Generated device list formats. The formats include the device name or IP address, and the device's SNMP access information. This information is used by Console to access and manage the device. You can mix SNMPv1/v2 and SNMPv3 formats in a single device list. If you list both an SNMPv1/v2 **and** SNMPv3 entry for a device, Console stores the v1/v2 values, but uses the v3 values to contact the device.

#### *SNMPv1/v2*

**NGF** lets you import a file that defines device name and SNMPv1/v2 security parameters for the device models being created by the import. The following parameters, separated by spaces, can be specified on each line within the import file to define a device. The minimum definition contains a device name (*dev=IP address*).

The following attributes are currently supported:



<b>Attribute</b>	<b>Description</b>	<b>Valid Parameters</b>
dev	Device IP Address (mandatory)	<IP address>
ro	Read-Only Community Name (optional) (see Note)	<community name>
rw	Read-Write Community Name (optional) (see Note)	<community name>
su	Super-User Community Name (optional) (see Note)	<community name>
mt	The poll type (monitor type) defined for the device (optional)	0 (Not Polled), 1 (Ping), 2 (SNMP)
pg	The poll group defined for the device (optional)	1, 2, or 3
cliDesc	A description of the CLI credential (optional)	<description>
cliUsername	The username used for device access (optional)	<username>
cliType	The communication protocol used for the connection (optional)	Telnet or SSH
snmp	The SNMP protocol version for the credential (optional)	v1, v2, or v3

SNMPv1/v2 access information consists of the read only, read write, and super user community names for devices. The device name or IP address is the only required information. The string of information for each device must be on a separate line with no line breaks in the string. If you create a device list without community names, devices will be imported into Console using the Default SNMPv1 profile defined in the Authorization/Device Access Window - Profiles/Credentials Tab.

Examples:

```
dev=Switch1 ro=public rw=public su=public
dev=172.16.30.40 ro=public rw=public su=public
dev=10.20.77.127 mt=2 pg=1 ro=public rw=public su=public
cliDesc=Default cliUsername=admin cliType=Telnet snmp=v1
```

**NOTE: For RoamAbout R2 devices.** If you are importing the device with SNMPv1 (SNMPv3 is recommended), the community names on the device must be updated. There are four SNMPv1 community names on the R2:

- Community #1 -- allows limited read-only access (MIB II system group)
- Community #2 -- allows limited read/write access (MIB II system group)
- Community #3 -- allows read-only access to all MIBs
- Community #4 -- allows read/write access to all MIBs

Console will import the device based on community names #3 and #4. For read-only access, set community name #3 on the device and then use that community name for the "ro" value in the device list. For read/write and super user access, set community name #4 on the device, and then use that community name for the "rw" and "su" values in the device list

### SNMPv3

SNMPv3 access information can consist of the following settings. The device name or IP address and the user name is the only required information. Each device must be on a separate line.

Attribute	Description	Valid Parameters	Co-requisite Attributes
dev	Device IP Address (mandatory)	<IP address>	NA
user	User (optional)	<username> <sup>1</sup>	NA
seclevel	Security Level (optional)	NoAuthNoPriv	NA
		AuthNoPriv	authtype, authpwd
		AuthPriv	authtype, authpwd, privtype, privpwd
authtype	Authentication Type (optional)	MD5	seclevel, authpwd
		SHA1	seclevel, authpwd

Attribute	Description	Valid Parameters	Co-requisite Attributes
authpwd	Authentication Password (optional)	<password> <sup>1</sup>	seclevel, authtype
privtype	Privacy Type (optional)	DES	seclevel, privpwd, authtype, authpwd
privpwd	Privacy Password (optional)	<password> <sup>1</sup>	seclevel, privtype, authtype, authpwd

1. Although SNMPv3 supports user names and passwords containing spaces, the NetSight Generated Format does not. When spaces occur in the user names and passwords in a .ngf file they are interpreted as a delimiter between parameters. For more information on SNMPv3, read RFC2574.

Examples:

```
dev=172.16.17.18 ro=public rw=private
dev=172.16.17.38 user=netmgr seclevel=AuthPriv authtype=MD5
authpwd=net_mgr.pwd privtype=DES privpwd=secret.pwd
```

## How Credentials and Profiles are Handled when Importing a Device List

*From NetSight Console*

When the import (from a .ngf file or remote Console) defines a device using SNMPv3 parameters that match a credential that exists in the local database, then the device is created using the existing Credentials and a Profile that is associated with them.

Otherwise, a new Profile is created, named *New* (default name) with the User Name (`user`), Security Level (`seclevel`), Authentication Type (`authtype`) and Privacy Type (`privtype`) and Passwords (`authpwd` and `privpwd`) from the import. The Credential that is created will be used for all Access Levels (Read, Write, Max Secure).

- If the Credential is created with an `authtype` and a `privtype`, the Profile is created with **AuthPriv** for all Access Levels.
- If the Credential is created with an `authtype`, but no `privtype`, the Profile is created with **AuthNoPriv** for all Access Levels.
- If the Credential is created with neither an `authtype` nor a `privtype`, the Profile is created with **NoAuthNoPriv** for all Access Levels.

### *From Ridgeline*

When importing a database backup file from Ridgeline, Credentials and Profiles are created based on the existing Credentials and Profiles in the Ridgeline database.

Instructions on:

- [Exporting a Device List](#)
- [Importing a Device List from a File](#)

## Exporting a Device List

### *From NetSight Console*

The Export option in NetSight Console creates a device list in NetSight Generated Format.

To export a device list:

1. Pull down the **File** menu and select **Device List > Export** from the menu. A file browser window opens where you can name your exported device list and navigate to a folder/directory where you want to place the file.
2. Type a name for your export file and click **OK**. Console exports all devices that have an SNMP Profile. Ping only devices are not exported.

### *From Ridgeline*

The backup utility in Ridgeline makes a backup copy of all data in the database. Database utilities are found in the `database\bin` directory in the folder in which you installed the Ridgeline software. For example, if you installed Ridgeline in the `C:\Program Files\Ridgeline`, the database utilities are saved in the `C:\Program Files\Ridgeline\database\bin` folder.

## Importing a Device List from a File

This feature imports device information and profiles for unique devices (ones that do not exist locally) from a .ngf or .sql file.

---

**NOTE:** Although SNMPv3 supports user names and passwords containing spaces, the NetSight Generated Format does not. When spaces occur in the user names and passwords in a .ngf file they are interpreted as a delimiter between parameters.

---

To import a device list:

1. Pull down the **File** menu and select **Device List > Import Devices** from the menu. A file browser window opens where you can navigate to a folder/directory containing the import file.
2. Select the import file and click **Import**. Devices that do not already exist in the database are added to the All Devices group and are assigned the Poll Group that has been designated as the default in the Status Polling view of the Suite-Wide Options window. If a device being imported exists in the local database, the local device information is retained and the import information about that device is ignored.

---

**NOTE:** In the .ngf file, when the parameters for a given device are invalid, the device will be created using the profile that has been designated as the default on the Authorization/Device Access Window - Profiles/Credentials Tab. Update and check the Console Event Log for specific information.

---

## Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)
- [Options Window](#)

For information on related tasks:

- [How to Add, Remove, and Delete Devices](#)
- [How to Add, Remove, and Rename Groups](#)

## How to Import ACL Data

---

To use ACL Manager, you need to import ACL data from your devices into ACL Manager. You can import ACL data from a Router Services Database file or from the devices you've modeled in Console. Imported ACLs are placed in folders labeled by IP address, under the Imported ACLs folder in the [ACL Editor](#) left-panel tree. The import operation also imports device interface and agent ACL assignment information into the ACL Manager's [interface assignment](#) and [agent assignment](#) views.

There is a possibility that imported ACLs will be duplicates of ACLs currently in the database. When this happens, it's important to understand how ACL Manager handles the imported ACLs. (ACLs with the same name and the same rules are considered to be duplicate ACLs.) By default, ACL Manager will search the Cataloged ACLs folder and the device-specific Import folder (and subfolders) for matches and create new ACLs only when there is no match. However, if a match is found, the matched ACL is used wherever that ACL is assigned. There are ACL Manager options that allow you to change the default import behavior and allow duplicate ACLs to be created. See the Help topic for [ACL Manager options](#) for more information.

If you import ACLs that have the same name but different rules, the ACLs will be created with a bracketed number. For example:

---

```
First_ACL
First_ACL [1]
First_ACL [2]
```

---

Instructions for:

- [Importing ACL Data From Devices](#)
- [Importing ACL Data From an RSD File](#)

### Importing ACL Data From Devices

Perform the following steps to import ACLs from one or more devices that you've modeled in NetSight Console:

1. In Console, select the devices in the left-panel tree.
2. Right-click on the devices and select **Import Device ACL Data**.

3. ACLs are imported into device-specific folders under the Imported ACLs folder in the [ACL Editor](#) left-panel tree. By default, ACL Manager dynamically checks for duplicate ACLs, comparing the imported ACLs against ACLs already within device-specific folders. When duplicate ACLs are found, they are not imported and ACL Manager uses the existing ACL. (There are ACL Manager options that allow you to change the default import behavior, and allow duplicate ACLs to be created. See the Help topic for [ACL Manager options](#) for more information.) The import operation also imports device interface and agent ACL assignment information into the ACL Manager's [interface assignment](#) and [agent assignment](#) views.

---

**TIP:** To import only the device interface and agent ACL assignment information into the ACL Manager, use the Refresh Device Data option available from the right-click menu off a device.

---

## Importing ACL Data From an RSD File

1. Click on the menu button  at the top left of the ACL tab and select **Import From RSD**. The **RSM Data Importer** window opens.
2. Navigate to the Router Services Manager Data file (.rsd file) and click **Open**. The ACL data is imported into the ACL Manager database.

---

### Related Information

For information on related tasks:

- [How to Manage ACLs](#)

## How to Manage ACLs

---


ACLs are the containers for the rules that govern network access through your routers. Traffic that arrives at a router port is either accepted or blocked according to the rules contained in an Access Control List (ACL). The ACL is examined from top to bottom, with the first rule that matches the packet determining the fate of that packet (dropped or forwarded). If there are no matching rules, the packet is denied. To change this behavior, add a rule that permits everything as the last rule in the ACL.

Managing ACLs could involve one or more of the following tasks:

- [Creating an ACL](#)
- [Copying an ACL](#)
- [Moving an ACL](#)
- [Translating ACLs](#)
- [Renaming an ACL](#)
- [Editing an ACL](#)
- [Deleting an ACL](#)
- [Creating an ACL Folder](#)

### Creating an ACL

Use these steps to create an ACL in the Cataloged ACLs folder:

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, expand the Cataloged ACLs folder and select the folder where you want to create the ACL.
3. Right-click on the folder and select **Create ACL <ACL Type>**.
4. Type the name for your new ACL and click **OK**. ACL names must be alphanumeric characters only and cannot include spaces. The new ACL appears in the left-panel tree.




**NOTE:** When ACL Manager enforces an ACL to a device, the name of the ACL on the device may not be the same as it appears in ACL Manager. ACL Manager attempts to use the same name on the device whenever possible. However, in certain situations a different name will be used. Because of this, an ACL may have a different name on each device it is enforced to. A different name will be used in the following circumstances:

- If the ACL name is non-numeric and the device only supports numeric names, or if the name is otherwise invalid on the device.
- If the name is in the Standard ACL range (1-99) but the ACL is an extended ACL, or if the name is in the Extended ACL range (100-199) but it is a Standard ACL.
- If another ACL with the same name already exists on the device.
- If the same ACL already exists on the device but with a different name, then the existing ACL will be maintained rather than creating a new one.
- The same ACL may have a different name on the device each time it is enforced. If its rules have been changed, it is more efficient to update the device in a way that does not preserve the name.

- 
5. Select the Description tab in the right panel and type a description for the new ACL.
  6. Select your new ACL in the left panel and [add rules](#).


## Copying an ACL

Sometimes its easier to start with an ACL that nearly matches your needs, than to create a new one from scratch. In those situations, you can copy an ACL from one location and paste it to another, then redefine one or more of its rules to create a new ACL.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, expand the folders and select the ACL being copied.
3. Right-click on the ACL and select **Copy** from the menu.
4. Right-click on the destination folder (the Cataloged ACLs folder or sub-folder) and select **Paste** from the menu.
5. [Edit](#) the ACL as needed.

## Moving an ACL

You can move ACLs from one location to another within the Cataloged ACLs folder using drag-and-drop or cut-and-paste.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. In the left-panel tree, expand the folders to select the ACL being moved and see its destination.
3. Move the ACL to the destination folder (the Cataloged ACLs folder or sub-folder) using drag-and-drop or cut-and-paste.

## Translating ACLs


ACL Manager lets you translate ACLs between the five supported ACL types (X-Series, N-Series 6.x, S/K/N 7.x+, XSR, and Common). When ACLs have been copied or cut, you can paste and translate them into a target location in the Cataloged ACLs folder as a different ACL type. When there is no direct translation from one type to another, the [ACL Translation View](#) lets you review the resulting ACL prior to translation. To translate an ACL:

1. **Copy** or **Cut** an ACL from the left-panel tree in the [ACL Editor](#). To cut or copy multiple ACLs, use the right-panel ACL Details tab.
2. Select a target location in the Cataloged ACLs folder where you want to paste the translated ACL, right-click and select **Paste and Translate <ACL type>**. The ACL type selected determines the ACL type following translation.
3. If there are no conflicts in the translation, the translated ACLs are pasted to the target location in the Cataloged ACLs folder. If conflicts are detected, the ACL Translation View opens where you can make decisions about how the translation will be performed. The top section lists the ACLs where a conflict was detected. The lower-left panel shows the rules for the ACL selected in the top panel with their original parameters. The lower-right panel shows how the rules will be changed if translated. Rules where a conflict exists are marked in the lower-left panel with an exclamation mark in the list; select the rule to view a comment below that describes the nature of the conflict.

4. To resolve conflicts:
  - a. Select an ACL from the top panel and examine the lower-right potential translation results panel.
  - b. If you decide that the translation should not be performed on the selected ACL, remove the **Check** in the **Translate** column for this ACL in the top panel. Otherwise, leave the Translate column checked.
  - c. Repeat steps a and b as needed, until all ACL/rule conflicts have been resolved.
5. After you've reviewed all the ACLs for conflicts, click **OK**. The ACLs with the Translate column checked are translated and pasted into the target. ACLs where the Translate checkbox is not checked are not translated, but are also pasted into the target.

## Renaming an ACL

You can rename ACLs in the Cataloged ACLs folder, but not in the Imported ACLs folder. To rename an ACL:

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. Expand the Cataloged ACLs folder and select the ACL being renamed. Right-click on the ACL and select Rename ACL from the menu.
3. Type the name for your new ACL. ACL names must be alpha-numeric characters only and cannot include spaces. Click **OK**.

**NOTE:** When ACL Manager enforces an ACL to a device, the name of the ACL on the device may not be the same as it appears in ACL Manager. ACL Manager attempts to use the same name on the device whenever possible. However, in certain situations a different name will be used. Because of this, an ACL may have a different name on each device it is enforced to. A different name will be used in the following circumstances:


- If the ACL name is non-numeric and the device only supports numeric names, or if the name is otherwise invalid on the device.
  - If the name is in the Standard ACL range (1-99) but the ACL is an extended ACL, or if the name is in the Extended ACL range (100-199) but it is a Standard ACL.
  - If another ACL with the same name already exists on the device.
  - If the same ACL already exists on the device but with a different name, then the existing ACL will be maintained rather than creating a new one.
  - The same ACL may have a different name on the device each time it is enforced. If its rules have been changed, it is more efficient to update the device in a way that does not preserve the name.
- 

## Editing an ACL

Editing ACLs consists of adding or [Deleting Rules](#) or [Rearranging](#) the order of existing rules. Refer to [How to Create Rules](#) to learn how to add rules to an ACL.


### *Deleting Rules*

In the ACL Editor, you can delete rules from the left-panel tree or from the right-panel Editor tab.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. Expand the left-panel tree as necessary and select the ACL where you are deleting the rule or rules.
3. Select the **Editor** tab in the right panel.
4. Select the rules being deleted from the table. Hold the **Shift** key while clicking to select consecutive rules from the table or hold the **Control** key to select non-consecutive rules.
5. Click the right-panel **Delete** button.


## Rearranging Rules

The order of rules in an ACL determines how packets will be managed. The ACL is examined from top to bottom, with the first rule that matches an incoming packet determining the fate of that packet (dropped or forwarded) according to the action specified in the rule.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. Expand the left-panel tree as necessary and select the ACL where you are rearranging rules.
3. Select the **Editor** tab in the right panel.
4. Select the rule being moved.
5. Click the **Move Up** or **Move Down** buttons to change the position of the rule. You can also click **Move To**, enter an index number, and press **Enter**.

## Deleting an ACL


ACLs can be deleted from any folder in the [ACL Editor](#) left panel tree or from the right-panel ACL Details tab.

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
2. Expand ACL folders as necessary and select the ACL being deleted from either the left panel tree or the right-panel ACL Details tab.
3. Right-click on the ACL and select **Delete** from the menu.

## Creating an ACL Folder

ACL Folders provide a container for managing ACLs. They let you create administrative groups of ACLs, such as ACLs that are applied to specific areas of your network or ACLs that may have similar parameters. ACL folders can be created at any level in the Cataloged ACLs folder in the ACL Editor left-panel tree, including in another ACL folder. However, aside from organizing folders and ACLs into a logical order, there is no inheritance or other significance to the hierarchy.

To create an ACL Folder:

1. In the ACL Manager tab, open the [ACL Editor](#) by clicking .
  2. In the left-panel tree, expand the Cataloged ACLs folders as necessary, and select the location for the folder.
  3. Right-click and select **Create Folder**.
  4. Enter the ACL folder name and click **OK**. The new folder is created. Empty folders will be deleted when you close the ACL Editor.
- 

### **Related Information**

For information on related windows:

- [ACL Editor](#)

For information on related tasks:

- [How to Create ACL Rules](#)

## How to Save and Restore Configuration Files

---

The Configuration Upload/Download window provides a way to upload configuration files from devices to save them elsewhere as backups, or restore configuration files by downloading the files to devices. Using these functions, you can copy configuration files from one device to another. On some devices, you can also use this window to save the bootlog file from a device. Files are transferred using TFTP; therefore, you must have a TFTP Server running to perform the upload or download.

---

**NOTES:** Console does not support Configuration Upload/Download for the RoamAbout R2.

This window is only available for devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

---

Instructions on:

- [Saving Configuration Files](#)
- [Restoring Configuration Files](#)
- [Saving Bootlog Files](#)

### Saving Configuration Files

Use the [Configuration Upload/Download window](#) to save a device's configuration file. This window is only available on devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

1. From the main Console window, right-click the device in the left panel and select **Configuration Upload/Download** from the menu. The Configuration Upload/Download window opens. (To open the window in Device Manager, select **Utilities > Configuration Upload/Download** from the Device View menu bar.)
2. In the Operations area, select the **Upload Configuration File from Device** option. This performs an upload of the device's active configuration file to a specified file on the TFTP server.
3. In the **Download Settings** area, specify the TFTP server to perform the upload operation. You can enter the TFTP server's IP address, or use the

dropdown list to select the server. The list displays IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.

4. If your TFTP server is configured with a root directory, select the **Server uses Root Path** checkbox, and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to upload the configuration file to this directory and any of its sub-directories. If the NetSight TFTP server is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Suite-Wide Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

5. In the **Full Image Path Field**, enter the full path and filename where you want to store the uploaded configuration file. You can also use the dropdown list to select a path and filename, or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a Root Path, the browse capability is limited to the directories below that root path.

---

**NOTE:** If you are creating a new file, browse to the directory and enter the new filename. The file will be automatically created as part of the upload operation as long as you are using the NetSight TFTP server. If you are using a different TFTP server, the new file will be created only if you are using a remote server and the full path is specified from the mapped drive.

---

6. The **Path to Set on Device** field displays the target path and filename as it will be set on the device. If the Server Uses Root Path checkbox is selected, the specified root path is stripped from the full path and filename. If the checkbox is not selected, this field displays the same path as the Full Image Path field.
7. Click **Apply** to initiate the upload operation and save the configuration file. For an explanation of status messages, see the [Configuration Upload/Download Window](#) Help topic.



## Restoring Configuration Files

Use the [Configuration Upload/Download window](#) to restore a configuration file to a device. This window is only available on devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

1. From the main Console window, right-click the device in the left panel and select **Configuration Upload/Download** from the menu. The Configuration Upload/Download window opens. (To open the window in Device Manager, select **Utilities > Configuration Upload/Download** from the Device View menu bar.)
2. In the Operations area, select the **Download Configuration File to Device**. This performs a download of a specified configuration file to the device.
3. In the **Download Settings** area, specify the TFTP server to perform the download operation. You can enter the TFTP server's IP address, or use the dropdown list to select the server. The list displays IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.
4. If your TFTP server is configured with a root directory, select the **Server uses Root Path** checkbox, and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to download files from this directory and any of its sub-directories. If the NetSight TFTP server is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Suite-Wide Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

5. In the **Full Image Path Field**, enter the full path and filename of the file you want to restore to the device. You can also use the dropdown list to select the full path and filename, or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a Root Path, the browse capability is limited to the directories below that root path.

6. The **Path to Set on Device** field displays the target path and filename as it will be set on the device. If the **Server Uses Root Path** checkbox is selected, the specified root path is stripped from the full path and filename. If the checkbox is not selected, this field displays the same path as the **Full Image Path** field.
7. Click **Apply** to initiate the download operation. For an explanation of status messages, see the [Configuration Upload/Download Window](#) Help topic.
8. The new configuration file is automatically activated following the download, except on devices supporting the *cfgGroup* MIBs. These devices require an additional operation in order to activate the new configuration file. If this is required, you will see an **Activate the Last Downloaded Configuration** option in the **Operations** area. To activate the configuration file on these devices:
  - a. In the **Operation** area, select the **Activate the Last Download Configuration** option.
  - b. Click **Apply** to activate the new configuration file.

## Saving Bootlog Files

Use the [Configuration Upload/Download window](#) to save a device's bootlog file. This operation is only available for devices supporting the *cfgGroup* MIBs.

1. From the main Console window, right-click the device in the left panel and select **Configuration Upload/Download** from the menu. The Configuration Upload/Download window opens. (To open the window in Device Manager, select **Utilities > Configuration Upload/Download** from the Device View menu bar.)
2. In the **Operations** area, select the **Upload Bootlog File from Device** option. This performs an upload of the device's bootlog file to a specified file on the TFTP server.
3. In the **Download Settings** area, specify the TFTP server to perform the upload operation. You can enter the TFTP server's IP address, or use the dropdown list to select the server. The list displays IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.
4. If your TFTP server is configured with a root directory, select the **Server uses Root Path** checkbox, and specify the root directory in the **Path** field (or use the **Browse** button to navigate to the directory). The root directory

is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to upload files to this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Suite-Wide Options window.

**NOTE:** When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

5. In the **Full Image Path Field**, enter the full path and filename where you want to store the uploaded bootlog file. You can also use the dropdown list to select a path and filename, or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a Root Path, the browse capability is limited to the directories below that root path.

**NOTE:** If you are creating a new file, browse to the directory and enter the new filename. The file will be automatically created as part of the upload operation as long as you are using the NetSight TFTP server. If you are using a different TFTP server, the new file will be created only if you are using a remote server and the full path is specified from the mapped drive.

6. The **Path to Set on Device** field displays the target path and filename as it will be set on the device. If the Server Uses Root Path checkbox is selected, the specified root path is stripped from the full path and filename. If the checkbox is not selected, this field displays the same path as the Full Image Path field.
7. Click **Apply** to initiate the upload operation and save the bootlog file. For an explanation of status messages, see the [Configuration Upload/Download Window](#) Help topic.

---

**NOTE: TFTP Configuration Upload** - When saving a configuration or bootlog file to a new file, Console's TFTP server always creates a new file during the save operation. If you are using a different TFTP server, one that requires that a new file is not automatically created, you should contact Extreme Networks Support at <http://www.extremenetworks.com/support/> for information on how to disable this feature.

---

## Related Information

For information on related windows:

- [Configuration Upload/Download Window](#)

For information on related tasks:

- [How to Download Firmware](#)

## How to Set Console Options

---

Use the Options window (**Tools > Options**) to set options for the NetSight Console application. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Console folder in the tree to view all the different options you can set.

Instructions on the following Console options:

- [Device Manager](#)
- [Discover](#)
- [FlexView](#)
- [Welcome View](#)
- [Property View](#)
- [Compass](#)
- [VLAN View](#)
- [Basic Policy View](#)
- [Wireless Manager](#)
- [Wireless Advanced Services](#)
- [Policy Control Console](#)
- [RoamAbout Wireless Manager](#)
- [TopN Collector](#)
- [NetFlow Collection](#)
- [OneView](#)
- [OneView Dialog Boxes](#)
- [OneView Collector](#)
- [OneView Engine](#)
- [ACL Manager](#)

### Device Manager

Device Manager options let you specify the polling cycles used to contact the device and update Device View information. These options apply only to the

NetSight Console Device Manager application.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Device Manager. The right-panel [Device Manager view](#) is displayed.
3. In the **Interval Between Poll Cycles** field, enter the amount of time (in seconds) that Device Manager waits between polling the device.
4. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
5. Click **OK** to set the options and close the window.

## Discover

Discover options let you specify options for the Console Discover operation. These options apply only to the NetSight Console application.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Discover. The right-panel [Discover](#) view is displayed.
3. 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. The default setting for Discover is 500.
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 is displayed in the Sample table scheme to the right of your selections.
5. Click **OK** to set the options and close the window.

## FlexView

FlexView options let you specify polling options for web-based FlexViews accessed through the OneView application's **Network** tab. These settings will apply to all users. The FlexView options also let you specify options for FlexViews accessed through Console. 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 Console folder and select FlexView. The right-panel [FlexView view](#) is displayed.
3. In the **For All Users** section, set the SNMP polling options for web-based FlexViews accessed through the OneView application's **Network** tab. The NetSight server polls the devices listed in the **Network** tab for FlexView table and graph information.
  - a. Set the **Maximum number of devices to contact at once**. This is the maximum number of IP addresses that the NetSight server will attempt to contact simultaneously. The NetSight server polls blocks of IP addresses, starting a new block each time the outstanding block completes.
4. In the **For Current User** section, set the options for FlexViews accessed through Console. Console polls the devices in a selected group (in the left-panel tree) for the FlexView table and graph information.
  - 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. The default setting for FlexViews is 500.
  - b. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
  - c. Set the **Export Directory** for your automatic FlexView exports. In FlexView Properties, you can configure FlexView table information to be automatically exported with each table refresh, using the Export Type parameter. The exported information is saved by default to the directory specified here.
5. Set the Advanced Editor option. The **Use OID Name** option specifies that the OID name will be used instead of the numeric OID in the XML encoding for the FlexView. Deselecting this option lets you create FlexViews with OID-based SNMP columns that are unique.
6. Click **OK** to set the options and close the window.

## Welcome View

The Welcome View option lets enable or disable the display of the right-panel **Welcome** tab. The **Welcome** tab is available when the top-level My Network folder is selected in the left-panel tree. It provides links to Console tasks such as

NetSight Discover and Authorization/Device Access windows, and also provides access to video tutorials on these tasks.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Welcome View. The right-panel [Welcome View](#) is displayed.
3. Use the checkbox to enable or disable the display of the Welcome View.
4. Click **OK** to set the option and close the window.

## Property View

Property View options let you specify options for the different views in the Console's **Properties** Tab.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Property View. The right-panel [Property View](#) is displayed.
3. 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. The default setting for Property View is 500.
4. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme below.
5. Click **OK** to set the options and close the window.

## Compass

Compass options let you specify Compass SNMP and Search options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Compass. The right-panel [Compass view](#) is displayed.
3. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the sample table scheme to the right of your selections.
4. The **Search Options** tabs determine which data sources will be used with



Compass searches. By default, Compass is configured to include the NAC Manager database (the "Network Access Control" checkbox) as well as various SNMP MIB objects when performing searches. (Refer to the [MIB/Table Descriptions](#) topic for information about MIB selections.) The Compass search begins by resolving IP address to MAC address in order to start searching for MAC-IP pairs from the network. When a match is found in the NAC Database, the SNMP MIBs will **not** be searched unless the "Search SNMP MIBs with database Match" checkbox is also selected. If the "Network Access Control" checkbox is deselected, then the NAC Manager Database will not be used to resolve IP address to MAC address. You can specify search options in three different tabs:

- **For all Users** - These search options will apply for all users on all NetSight clients.
  - **For Current User** - These options let you override the All Users search options and instead use this set of search options for the current user. These settings are stored in the user's home directory and will apply only to the NetSight client running on this machine or machines with shared access to the user's home directory.
  - **OneView** - These options are for the Compass search in Extreme Management Center. In addition to search options, they include search limit settings which are used to help limit the NetSight server resources used for the searches:
    - **Number of searches allowed at once.** The maximum number of OneView Compass searches that can be performed at one time.
    - **Number of search results allowed.** The maximum number of search results that can be displayed in the table.
    - **Number of devices allowed for a search.** The maximum number of devices that can be included in a search.
    - **Time limit for a search.** The maximum search time in seconds.
5. Click **OK** to set the options and close the window.

## VLAN View

VLAN options let you specify options for the VLAN views. These options apply only to the NetSight Console application.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select VLAN. The right-panel [VLAN View](#) is displayed.
3. 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. The default setting for VLAN is 500.
4. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
5. Select the **Enable Display of Port Elements** checkbox to filter the port views based on selected port elements, making it easier to use VLAN Manager with groups of port elements.
6. Specify the **Default VLAN Port Sort**. Use the radio buttons to specify how the data in the **VLAN Basic Port** tab will be sorted by default when the device data is retrieved: by IP address and Port, by IP address and Name, or by the sort used by the last user. The "By Last User Sort" option allows you to continue to use the last sort options you had configured using the Sort Toolbar (available from the right-click menu on a table entry). For example, if you had the sort set to Port (descending) and PVID (ascending) and you close the application, then the next time you open the application, the tab uses the same sort.
7. Click **OK** to set the options and close the window.

## Basic Policy View

Basic Policy View options let you specify options for the different views in the Console's **Basic Policy** Tab.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Basic Policy View. The right-panel [Basic Policy View](#) is displayed.
3. 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 **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your

selection will be displayed in the Sample table scheme below.

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

## Wireless Manager

Wireless Manager options let you specify options for the Wireless Manager application.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Wireless Manager. The right-panel [Wireless Manager view](#) is displayed.
3. In the **Wireless Advanced Services** section, enter the IP address of the Wireless Advanced Services server. This server requires additional licenses to operate.
4. Enter the **Default Shared Secret**. Any time NetSight discovers a new controller, Wireless Manager will attempt to authenticate with the controller using this shared secret. For proper functioning of OneView, Wireless Manager, and Wireless Advanced Services, the controller must be configured with the same shared secret as Wireless Manager. Each controller can be configured with a different shared secret as long as Wireless Manager knows what it is. You can configure Shared Secrets on a per controller basis using Wireless Manager. Please refer to the Wireless Manager online Help for additional details.
5. Enter the **Maximum Number of Executed Tasks to retain in Task History**. After a task has executed, it is retained in the Wireless Manager database to provide a detailed history of task activity. A large amount of information is kept for each executed task, including the complete CLI script executed against each target controller. To maintain the database at a reasonable size, Wireless Manager keeps only a fixed number of executed tasks in the database. When the task limit is reached or exceeded, Wireless Manager deletes the oldest executed tasks from its database. The History option allows you to control how many task definitions Wireless Manager will retain in its database. The default is 100 executed tasks retained, and the maximum is 500 tasks retained.
6. Enter the **Audit Start Time** and **Audit Interval**. Wireless Manager audits controller configuration to ensure that it does not deviate from the deployed templates. When Wireless Manager encounters discrepancies between the template and the actual controller configuration, the audit feature logs an error. You can manually run an audit or you can schedule

automatic audits using the Audit options. Select the time of day when the audit should start and the interval in hours between the start of successive audits. Auditing once every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

7. Select the **Table Colors**. You can customize the appearance of the screens in Wireless Manager by applying contrasting colors to alternating table rows. From the drop-down menu, select row colors for alternating primary and secondary rows. A sample to the right provides a snapshot of the way table colors will display on the screen.
8. Click **OK** to set the options and close the window.

## Policy Control Console

These options let you define the SNMP polling parameters for the Policy Control Console (PCC) tool and the authorization group for the PCC appliance.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Policy Control Console. The right-panel [Policy Control Console view](#) is displayed.
3. Use the drop-down list to select the **Appliance Authorization Group** that uses the correct profile for the PCC appliance to use when communicating with devices. Profiles define the level of device access granted to users that are members of that Authorization Group. Profiles and Authorization Groups are defined in the Authorization/Device Access window (Tools > Authorization/Device Access).
4. Click **OK** to set the options and close the window.

## RoamAbout Wireless Manager

RoamAbout Wireless Manager options let you specify which right-panel tabs you want displayed in the RoamAbout Wireless Manager main window.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select RoamAbout Wireless Manager. The right-panel [RoamAbout Wireless Manager view](#) is displayed.
3. Select the desired checkboxes to specify which right-panel tabs you want displayed in the RoamAbout Wireless Manager main window.
4. Click **OK** to set the options and close the window.

## TopN Collector

The TopN Collector collects the data used in OneView TopN reports. It also collects the signal strength data reported by Wireless Controllers.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select TopN Collector. The right-panel TopN Collector view is displayed.
3. Use the checkbox to enable or disable TopN collection.
4. Select the **Host Name Resolution** option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for TopN only. (Host name resolution is enabled globally using the Suite Name Resolution option.) Changes to this option take place immediately.
5. Specify the number of days to maintain the TopN history. This setting determines how many days of TopN information will be available for viewing in the reports. The default number of days is 30, with a minimum value of 1 day and a maximum value of 180 days.
6. Click the **Advanced Settings** button to open the [TopN Collector Advanced Settings window](#) where you can configure advanced TopN Collector options.
7. Click **OK** to set the options and close the window.

## NetFlow Collection

NetFlow options let you configure NetFlow flow collection settings.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select NetFlow. The right-panel [NetFlow Collection view](#) is displayed.
3. Use the **Enable NetFlow Collector** checkbox to enable/disable NetFlow packet processing on the NetSight server, allowing you to turn off NetFlow for troubleshooting purposes. When NetFlow is enabled or disabled, a message is logged to the Console log as well as the NetSight server log. When NetFlow is disabled, the Application Flows report on the OneView **Flows** tab is cleared. However, the Flow Engine Summary on the OneView **Administration** tab continues to show the statistics for previous flows.

4. Changing the value in the **Maximum Flows to Maintain in Memory** field would adjust the amount of memory used to store flows.
5. Changing the value in the **Maximum Aggregate Flows to Maintain in Memory** field would adjust the amount of memory used to store aggregated flows.
6. The **Maximum Number of Flows Allowed per Table View** number sets the maximum number of flows that can be displayed in OneView NetFlow reports.
7. The **Send/Receive NetFlow Data on Socket** is the port on the NetSight server that listens for flow collection data. If you change this port number here, you will also need to reconfigure the port number on the switch.
8. The **Export Interval** is the active timer which determines the maximum amount of time a long-lasting flow will remain active before expiring. When a long-lasting active flow expires due to the active timer expiring, another flow is immediately created to continue the ongoing flow. The NetSight flow collector rejoins these multiple flow records to report a single logical flow.
9. The **Template Refresh Rate** is the number of export packets sent before the flow sensor retransmits a template to the collector when using NetFlow Version 9.
10. The **Template Timeout** is the number of minutes the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.
11. Select the **NetFlow Host Name Resolution** option to resolve host names to IP addresses and IP addresses to host names, if possible. This option enables host name resolution for NetFlow only. Host name resolution for the NetSight Suite is enabled globally using the NetSight Suite-Wide Name Resolution option. The Suite-Wide option must be enabled for this NetFlow option to take effect.
12. Select the **NetFlow Port Name Resolution** option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to disable port name resolution for NetFlow only. (Port name resolution is enabled globally using the Suite Name Resolution option.)
13. Click the **Advanced Settings** button to open the [NetFlow Advanced Settings window](#) where you can configure advanced settings for NetFlow flow collection.
14. Click **OK** to set the options and close the window.

## OneView

The OneView options let you specify SNMP polling options for the real-time data collection used in the OneView Search (PortView) **Overview** tab.

You can also adjust the maximum number of **FlexView** or **PortView** tabs that can be displayed in OneView at one time. For example, the default limit of five PortViews allows you to have five active searches open at one time. Changing the limit to ten would allow you to have ten active searches open at one time. Keep in mind that adjusting these settings to a higher number could impact OneView performance.

You can also use this view to set the Date and Time format to be used in OneView reports.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select OneView. The [OneView](#) panel is displayed.
3. Use the drop-down menu to select the **Poll Interval**, which is the amount of time (in seconds) that OneView waits between polling the device.
4. Set the desired **session limits**. These settings specify the maximum number of **FlexView** and **PortView** tabs per NetSight server that can be displayed in OneView at one time. Adjusting these settings to a higher number could impact OneView performance.
5. Select the option that formats the date -- day (DD), month (MM), and year (YYYY) -- according to your personal preference. Select the option that formats the time -- 12-hour or 24-hour clock -- according to your personal preference.
6. Specify how you want to display end-system MAC addresses in the OneView Wireless client and threat tables, as well as the **Control** tab End-System 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".
7. In the **Map Settings** section, change the Status Refresh Interval, if desired. OneView maps display an integrated alarm/device status either to the right

of a device or AP image, or incorporated as part of a map marker. The alarm status automatically refreshes every 30 seconds by default. Use the drop-down list to change the refresh interval. This option provides a way to adjust the load on the NetSight server if status requests are causing performance issues. You can change the setting to a longer interval or to None, as your situation requires.

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

## OneView Dialog Boxes

The OneView Dialog Boxes option lets you re-show all message dialog boxes that you have turned off in OneView (for example, if you have selected the "Do not show this message again" checkbox on a Warning dialog). This setting applies only to the current user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select OneView Dialog Boxes. The right-panel [OneView Dialog Boxes view](#) is displayed.
3. Click the **Re-show All** button.
4. Click **OK** to set the option and close the window.

## OneView Collector

OneView Collector options let you specify SNMP polling options for OneView data collection, enable and disable wireless statistics collection, and access advanced settings for the OneView Collector.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select OneView Collector. The right-panel [OneView Collector view](#) is displayed.
3. In the **Wireless Collection** section, use the **Collect Statistics** checkbox to enable or disable wireless data collection.
  - a. In the **Access Point Poll Rate** field, enter the amount of time (in minutes) that the data collector waits between polling wireless access points. Valid values are 1-60 minutes.
  - b. In the **Controller Poll Rate** field, enter the amount of time (in minutes) that the data collector waits between polling wireless controllers. Valid values are 1-60 minutes.



- c. Use the **Edit Include/Exclude Filter List** option to filter the client events displayed in the OneView Wireless Client History, Top Clients by Bandwidth, and Client Event History reports. Click the **Edit** button to open a window where you can use the drop-down list to select whether to display client events for:
    - All SSIDs and Topologies** - Client events for all SSIDs and Topologies will be displayed.
    - Some SSIDs** - Select the SSIDs to include or exclude.
    - Some Topologies** - Select the Topologies to include or exclude. The Client Event History report does not support the ability to filter on topologies.
  - d. Use the **Edit Client History and Rogue AP** option's **Edit** button to open a window where you can configure Wireless History Settings. These settings pertain to the OneView Wireless Client Event History report.
4. In the **Device Collection** section, use the **Collect Statistics** checkbox to enable or disable device data collection.
  - a. Use the **Collect Additional Extreme/Enterasys Statistics** checkbox to enable or disable Extreme or Enterasys switch resource statistics collection.
  - b. Use the **Collect Host Resource Statistics** checkbox to enable or disable host resource statistics collection.
  - c. In the **Poll Rate** field, enter the amount of time (in minutes) that the data collector waits between polling devices. Valid values are 1-60 minutes.
5. In the **Interface Collection** section, use the **Collect Statistics** checkbox to enable or disable interface data collection.
  - a. Use the **Collect Additional Extreme/Enterasys Statistics** checkbox to enable or disable Extreme or Enterasys interface statistics collection.
  - b. In the **Poll Rate** field, enter the amount of time (in minutes) that the data collector waits between polling interfaces. Valid values are 1-60 minutes.
6. In the **NAC Collection** section, use the **Collect NAC Statistics** checkbox to enable or disable NAC data collection.
  - a. In the **Poll Rate** field, enter the amount of time (in minutes) that the data collector waits between polling NAC appliances. Valid values are 1-60 minutes.

7. Click the **Advanced Settings** button to open the [OneView Collector Advanced Settings window](#) where you can configure advanced settings for the OneView data collector.
8. Click **OK** to set the options and close the window.

## OneView Engine

OneView Engine options let you specify data aging options and advanced settings for data archiving and aggregation.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select OneView Engine. The right-panel [OneView Engine view](#) is displayed.
3. Set the **Data Aging** options. Data aging options determine how long the collection data used by OneView reports is maintained in the OneView database. You can set an aging value for each of the following data types:
  - collection data - This setting specifies how long (in days) to maintain the raw data collected by the OneView data collector. Valid values are 1-1000 days.
  - hourly data - Every hour, the raw data is condensed into hourly average values and archived. This setting specifies how long (in weeks) to maintain the archived hourly data. Valid values are 1-800 weeks.
  - daily data - Every day, the hourly data is condensed into daily average values and archived. This setting specifies how long (in months) to maintain the archived daily data. Valid values are 1-200 months.
  - weekly data - Every week, the daily data is condensed into weekly average values and archived. This setting specifies how long (in months) to maintain the archived weekly data. Valid values are 1-200 months.
  - monthly data - Every month, the weekly data is condensed into monthly average values and archived. This setting specifies how long (in months) to maintain the archived monthly data. Valid values are 1-200 months.
4. Set the **Server CPU Reporting** interval. OneView collects NetSight server CPU usage statistics to monitor how busy the NetSight server is. At 5 minute intervals (the default interval) the collected usage data is averaged, and the average and maximum statistics are reported to the OneView

database to provide data for the OneView NetSight Server CPU Utilization report. You can change the default interval setting here, if desired. A shorter interval would provide a more granular picture of CPU usage while a longer interval would mean that less data is stored in the database. Valid values are 1-59 minutes.

5. Click the **Advanced Settings** button to open the [OneView Engine Advanced Settings window](#) where you can configure advanced data archiving, data aggregation, and session limit options.
6. Click **OK** to set the options and close the window.

## ACL Manager View

ACL Manager options let you specify options for the **ACL Manager** tab.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select ACL Manager. The right-panel [ACL Manager View](#) is displayed.
3. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
4. In the **Well-Known Identifiers** section, select the checkbox if you would like to show the well-known identifier protocol when displaying ACL rules in the **ACL Editor** tab.
5. In the **ACL CLI Preview Indices** section, select the checkbox if you would like to display line numbers in the **ACL Editor CLI Preview** tab.
6. In the **Detail Log** section, select the checkbox if you would like to have the ACL Manager Detail Log automatically cleared when NetSight Console is restarted.
7. In the **Import ACLs From Device** section, use the checkboxes to select the following parameters when performing an ACL import from a device:
  - **Create New ACLs** - ACL Manager compares the imported ACLs against ACLs already within the Catalog folder and device-specific folders, checking for duplicates. If a duplicate ACL is found, the ACL is not imported and ACL Manager uses the existing ACL. If a duplicate ACL is **not** found and this option is selected, a new ACL is created in the ACL Manager database. If this option is not selected, a new ACL will not be created.

- **Match ACLs in Catalog** - Use this option to specify whether or not ACL Manager will compare imported ACLs against ACLs already within the Catalog folder.
  - **Match ACLs in Device-Specific Folder** - Use this option to specify whether or not ACL Manager will compare imported ACLs against ACLs already within the device-specific folders.
8. In the **Enforce** section, use the checkboxes to select the following Enforce operation parameters:
- **Include Save Active to Startup** - When this options is selected, the Enforce operation saves the Active Configuration to the Startup Configuration for the selected device. The default setting is checked.
  - **Allow ACLs to Deny NetSight** - When this option is selected, ACL Manager will no longer check for ACLs which deny access to the device from the NetSight server. Use of this option could result in lost contact with the device. If contact is denied by an ACL, you must use the device's command line interface (CLI) to remove the ACL and restore contact. The default setting is unchecked.
  - **Delete Unused ACLs** - When this option is checked, ACL Manager will delete any unused ACLs on devices where it performs an Enforce. ACL Manager considers ACLs that are currently defined on a device, but not currently applied to any interfaces or in use by other facilities on the device as Unused. The default setting is checked.
9. In the **Exclude ACL Range** section, you can define a range of ACLs that cannot be used by ACL Manager when allocating a new name for an ACL on a device. For example, let's say the excluded range is 101-103:
- If you create a new ACL named "new\_acl" and assign it to an interface on a device, when you enforce, ACL Manager determines that ACL "new\_acl" needs to be copied to the device. It also determines that "new\_acl" is an invalid name on that device because the device only supports numbered ACLs. Therefore, ACL Manager must assign a new name for the ACL on the device. The ACL is an extended ACL, and only ACLs 100-199 can be considered for extended ACLs. So, ACL Manager considers using 100. If 100 is already in use, ACL Manager will consider 101. But 101 is excluded. So ACL Manager will consider 102, 103, and finally 104. 104 is not used and not excluded, so it will be used as the new ACL name on the device.
  - If you create a new ACL named 102, and assign it to an interface on a device, when you enforce, ACL Manager determines that ACL 102

needs to be copied to the device. It also determines that 102 is an invalid name on that device because it is in the excluded range. Therefore, ACL Manager must assign a new name for the ACL on the device. The ACL is an extended ACL, and only ACLs 100-199 can be considered for extended ACLs. So ACL Manager will consider using 100. If 100 is already in use, ACL Manager will consider 101. But 101 is excluded. So ACL Manager will consider 102, 103, 104, and finally 105. 105 is not used and not excluded, so it will be used as the new ACL name on the device.

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

---

### **Related Information**

For information on related windows:

- [Console Options](#)

## How to Translate ACLs and Rules

---

ACLs and rules can be copied or cut from one location and pasted to another location in the ACL Editor left-panel tree. When pasting an ACL, you can select "Paste and Translate" to convert an ACL from one type to another. If the translation could result in a conflict, as when a particular rule type must be modified or removed, the ACL Translation View opens to allow you to review the impact of the translation. A similar thing happens with rules. When a conflict is detected for rules that are pasted from one ACL type to another, the Rule Translation View is automatically opened.

Instructions on:

- [Paste and Translate ACL\(s\)](#)
- [Translating Rules](#)

### Paste and Translate ACL(s)

You can translate ACLs from one type to another using the **Paste and Translate** menu option.

To paste and translate from one ACL type to another:

1. Select the ACL being translated from the ACL Editor left-panel tree. To select multiple ACLs use the right-panel ACL Details tab.
2. Right-click and select **Copy** or **Cut**.
3. Right-click on the Cataloged ACLs folder and select **Paste and Translate** to the desired ACL type.
4. If there are no incompatible rules within the ACL(s) being translated, then the translated ACLs are placed in the target location. If ACL Manager detects incompatible rules, the ACL Translation View automatically opens.
5. In the ACL Translation View, resolve the conflicts before continuing:
  - a. Select an ACL from the list in the upper section of the view. The two lower tables show the incompatible rules: on the left as they exist in the original ACL, and on the right as they will be translated. Rules that cannot be translated will be removed. Rules that can be translated with changes appear in the lower-right panel.

- b. Check the checkbox **Split all IP rules with source or dest ports into UDP/TCP rules** if you want to create two rules, one UDP and one TCP to replace IP rules that have ports specified.
  - c. After reviewing the resulting rules, decide whether or not to continue with the translation. If you decide not to translate the selected ACL, clear the check in the box in the **Translate** column.
  - d. Repeat Steps 5a through 5c until you've reviewed/resolved all of the ACLs being translated.
6. Click **OK**. ACLs that were checked for translation are translated and placed in the target location. ACLs that were unchecked are placed in the target location in their original form (no translation).

## Translating Rules

Pasting rules that have been copied or cut, or dragging a rule from one ACL type to another assumes that you are translating the rule(s) into a type that is compatible with the target ACL.

---

**NOTE:** It is recommended that you **Copy**, rather than **Cut** rules when translating, because the Copy option retains a copy of the rule in the paste buffer after pasting (translation). If you Cut a rule that is incompatible with the destination, the Rules Translation View opens to show how the Rule will be altered or dropped and your only choice is to click **OK**. This will translate the rule, which in some cases means dropping it and the rule is effectively removed.

---

To translate a rule:

1. Expand the ACL Editor left-panel tree and select the rule being translated. You can also select multiple rules by selecting an ACL in the left panel, then selecting one or more rules in the Editor tab.
2. Right-click on the rule and choose **Copy** or **Cut**. (You can also drag rules singly from one location to another in the ACL Editor left-panel tree or drag one or more rules from the Editor tab to a target ACL in the left-panel tree. This is effectively a Cut and Paste operation. Refer to the recommendation in the previous note.)
3. Right-click on the target ACL where you want to place the translated rules, and choose **Paste**.

4. If there are no incompatible rules being translated, then the translated rules are placed in the target location. If ACL Manager detects incompatible rules, the [Rule Translation View](#) automatically opens.
  5. Click **OK**. If the translation drops a rule that you've copied, you can paste it back into the original ACL.
- 

### **Related Information**

For information on related windows:

- [ACL Translation View](#)
- [Rule Translation View](#)



## How to Use Compass

---

Compass is a powerful search tool that provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations. You can use Compass to search one or more devices or device groups selected in the Console left panel. (If you do a search on a user-created group that contains interfaces, the whole device on which the interface is located will be searched.) The search is based on the following:

- the selection you make in the Console left panel ([Search Scope](#))
- the [Search Type](#) you select on the Compass tab
- the [Search Parameters](#) you provide on the Compass tab

The [Search Log tab](#) displays a log of the progress of the search and notifies you of unsupported devices. The [Results tab](#) displays the results of the Compass search. You can customize table settings and find, filter, sort, print, and export the information in the Search Log and Results tabs. Access these Table Tools through a right-click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic. (If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.)

Instructions on:

- [Accessing Compass](#)
- [Searching](#)
  - [All](#)
  - [Auto](#)
  - [IP Addresses](#)
  - [IP Subnet](#)
  - [MAC Addresses](#)
  - [Multicast Addresses](#)
  - [User Names](#)
- [Pinging](#)

## Accessing Compass

To access the Compass tab:

1. Open the My Networks folder in the left panel and select the device group (s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select a [Search Type](#) from the drop-down list.

## Searching

Compass enables you to search selected devices using several different search types.

### *Auto Searching*

The [Auto Search](#) auto-detects the address format you enter in the Search Parameters Address field, and performs the appropriate search.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select Auto from the Search Type drop-down list.
4. In the Address text field, enter an address or hostname, using any of the allowed [formats](#).
5. Select any desired [Results Filters](#) (you can also do this after the search is completed).
6. Click **Search**.
7. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
8. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching All*

The [All Search](#) finds any network element which is aware of the devices within the selected scope, and lists the addresses associated with them.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select All from the Search Type drop-down list.
4. Select any desired [Results Filters](#) (you can also do this after the search is completed).
5. Click **Search**.
6. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
7. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching IP Addresses*

The [IP Address Search](#) finds any device which is aware of the specified IP address/hostname within the selected scope, and lists the addresses associated with it.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select IP Address from the Search Type drop-down list.
4. To search for all IP address information within the selected scope, leave the "IP Address or Hostname" text field blank. To search for information on a specific IP address or hostname, enter it in the IP Address or Hostname text field.
5. Select any desired [Results Filters](#) (you can also do this after the search is completed).
6. Click **Search**.
7. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
8. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching IP Subnets*

The [IP Subnet Search](#) finds any device which is aware of the specified IP subnet within the selected scope, and lists the end stations in the IP subnet.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select IP Subnet from the Search Type drop-down list.
4. In the IP Address or Hostname text field, enter an IP address from the subnet whose members you want to find.
5. Select the [Subnet Mask](#) text field. This causes the text field to display the natural network mask. You can leave this, or enter a different network mask. The format of this text box depends on the format selected for the Suite-Wide Data Display Network Mask option in the **Tools > Options** window: either CIDR or dot-delimited. An example of the selected format is provided below the text box.
6. Select any desired [Results Filters](#) (you can also do this after the search is completed).
7. Click **Search**.
8. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
9. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching MAC Addresses*

The [MAC Address Search](#) finds any device which is aware of the specified MAC address within the selected scope, and lists the addresses associated with it.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select MAC Address from the Search Type drop-down list.
4. Choose one of the following:
  - To search for all MAC addresses within the selected scope, leave the "MAC Address" field blank.
  - To search for information on a specific MAC address within the selected scope, enter the specific MAC address on which you wish to search. You can also enter a partial address, to search for a specific vendor's equipment (e.g. 0 . 0 . 1 d). (See <http://standards.ieee.org/regauth/oui/oui.txt> for vendor MAC

address prefixes.) Formats allowed are dot, colon, space, dash, and no delimiter:

- 0.0.1d.1.2.3
- 00:00:1D:01:02:03
- 00 00 1D 01 02 03
- 00-00-1D-01-02-03
- 00001D010203

The vendor for the hardware associated with the MAC address you are entering appears here as soon as you type enough of the MAC address for Compass to recognize it.

5. Select any desired [Results Filters](#) (you can also do this after the search is completed).
6. Click **Search**. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
7. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching Multicast Addresses*

The [Multicast Address Search](#) finds any device which is aware of the specified multicast address within the selected scope, and lists the addresses associated with it.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select Multicast Address from the Search Type drop-down list.
4. Choose one of the following:
  - To search for all multicast addresses within the selected scope, leave the Multicast Address text field blank.
  - To search for information on a specific multicast address within the selected scope, enter the multicast address in the Multicast Address text field. See <http://www.iana.org/assignments/multicast-addresses> for a list of common multicast address groups. The description of the multicast address you are entering appears in the Description as soon as you type enough of the address for Compass to recognize it.

5. Select any desired [Results Filters](#) (you can also do this after the search is completed).
6. Click **Search**. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
7. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

### *Searching User Names*

The [User Name Search](#) finds any device which is aware of the specified user name within the selected scope, and lists the addresses associated with it.

1. In the left panel, select the device group(s) or device(s) that you want to search.
2. Select the Compass tab in the right panel.
3. Select User Name from the Search Type drop-down list.
4. To search for all user names within the scope, leave the User Name field blank. To search for information on a specific user name within the selected scope, enter the user name. You can also enter a partial user name; for example, if you entered "tom" as your search criteria, "tommy" and "atom" would be found.
5. Select any desired [Results Filters](#) (you can also do this after the search is completed).
6. Click **Search**.
7. To view a log of the search progress, select the [Search Log tab](#) in the bottom section of the Compass tab.
8. View the results of the search in the [Results tab](#) in the bottom section of the Compass tab.

## **Pinging**

Use the following steps to ping an IP address to determine if the network element is contactable.

---

**NOTE:** On a Windows platform, ping will not work unless you are logged on and running Console as a user with Administrative privileges.

---

1. Select the Compass tab.
  2. Select IP Address from the Search Type drop-down list.
  3. In the "IP Address or Host Name" field, enter the IP address or host name for the network element you want to ping.
  4. Click **Ping Address**. The [Ping window](#) opens and the IP address is automatically pinged.
  5. View the results of the ping in the log.
  6. Click **Close** to leave the Ping window, or **Clear** to clear the data from the window and ping another network element. To ping another network element, enter its IP address or host name and click **Ping**.
- 

### Related Information

For information on related windows:

- [Compass Tab](#)
- [Ping Window](#)

## How to Use MIB Tools

---

With MIB Tools, you can examine the MIBs supported by an active device on your network, change the value of a writable MIB object, and add rows to MIB tables. The following sections detail how to contact a device, view its supported MIBs, query the device for MIB values, set a new value for a MIB object, and add rows to MIB tables on the device. For more information on MIBs, see [MIB Tools Overview](#).

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

To access MIB Tools, select **Tools > MIB Tools** from the Console menu bar, or right-click a device in the Console left panel and select MIB Tools from the menu.

Information on:

- [Contacting a Device](#)
- [Searching for MIB Objects](#)
- [Querying MIB Objects](#)
  - [Clearing Query Results](#)
- [Setting MIB Objects](#)
- [Adding Rows in MIB Tables](#)
- [Adding MIBs to the MIB Tools Database](#)

### Contacting a Device

If you have launched MIB Tools from a device selected in the Console's left panel, MIB Tools will automatically attempt to contact the device. Otherwise, you can contact a device using the Device and Select Protocol areas in the [MIB Tools window](#).

1. In the Device area, enter the device's IP address or select a previously contacted IP address from the drop-down list.



2. In the Select Protocol area, select the SNMP version and access properties you want MIB Tools to use to contact the device:
  - **Use SNMPv1** -- Select this option for SNMPv1 devices, and enter a community name or use the drop-down list to select a community name. The permissions assigned to the community name you enter here will determine the level of access you have to the device's MIB information: Read Only, Read-Write, or Superuser. Be sure to use a community name with the appropriate level of access.
  - **Use SNMPv3 Credential** -- Select this option for SNMPv3 devices and use the drop-down list to select a user name to contact a device. To create or edit a Console credential, click **Edit** to open the [Edit Credentials window](#).
  - **Use Console Profile** -- Select this option to use a Console Profile and use the drop-down list to select a profile. To create or edit a profile, click **Edit** to open the Authorization Configuration/Device Access Window - Profiles/Credentials Tab. Select the Use Max Access/SuperUser checkbox to specify max access/superuser access for all requests.
3. Click the **Contact** button or the [contact icon](#). Contact status is shown by the contact icon and in the status bar at the bottom of the window.

## Searching for MIB Objects

The MIB Tools' Find feature allows you to search the MIB Tree for objects matching specific text or an OID. The Find feature is located at the bottom of the [Tree tab](#).

1. In the **Find What** field, enter the MIB text name or OID you want to find.
2. Click the **Find** button. The search begins at the currently selected object in the MIB Tree. The first matching MIB object is highlighted (selected) in the MIB Tree and also the [List tab](#). In addition, the [Details tab](#) displays the corresponding MIB object information and the Find What and Current Object fields are updated to reflect the selected MIB object.
3. Click **Find** again to highlight the next matching entry. When the end of the tree is reached, the search begins again at the root of the MIB Tree.

---

**TIP:** Use the **Options** button to open the Options window where you can specify different attributes for the Find operation. For more information on Find options, see the Find Toolbar Options Help topic.

---

## Querying MIB Objects

To find the current value set at the selected device for a specific MIB object, you must query the device for the information. The query results appear in the [Results table](#) at the bottom of the window.

1. [Contact a device.](#)
2. In the MIB Tree display, select one of the following:
  - Select the leaf for a particular MIB object if you want to retrieve an individual value.
  - Select a Branch or Table folder, if you want to traverse the MIB and retrieve values for all objects within that portion of the MIB.You can also enter the folder or object's text name or OID in the Current Object field.
3. For objects with multiple instances, enter the instance number to be used for a Get request. For example, if you are querying a switch's interface table, there would be multiple instances (values) returned for each leaf object in the table (one for each port), and each instance would have a unique instance value appended to the object's OID.
4. Use the Request Type drop-down list to select the type of request to send to the selected device:
  - **GetNext** -- requests all the instances of the MIB object or folder specified in the Current Object field.
  - **Get** -- requests the first instance of the MIB object specified in the Current Object field.
  - **Single GetNext** -- requests the next single instance of the MIB object specified in the Current Object field.
5. Click the **Query** button. The Status Bar at the bottom of the window will inform you about the progress of your query. All values returned from the specified leaf or from all objects within a folder are displayed in the Results table. The Query button changes to **Stop** while a query is being performed. If you stop the query operation, the query will be cancelled, but all values returned before the query was stopped will remain in the Results Table.

### *Clearing Query Results*

The Auto Clear option, located above the Results table, determines how query results are cleared.

- If Auto Clear is not selected, the results of each query accumulate in the Results table until you remove all responses by clicking the **Clear** button.
- If Auto Clear is selected, the results of each query will automatically be erased each time you perform a new query operation.

## Setting MIB Objects

Use the Table Editor (the bottom row of the [Results table](#)) to change the syntax and/or value of a writable MIB object.

---

**TIP:** For more detailed information about a MIB object, select the object in the [Tree tab](#). The [Details tab](#) displays object information including a list of valid values for writable objects, along with the numerical code for each value.

---

1. Be sure that you have contacted the correct device and that you have selected the [protocol](#) which provides you with write access to the desired MIB object.
2. Query the device for the desired MIB object, as described in [Querying MIB Objects](#).
3. In the Results table, click on the object and instance of interest.
4. In the Table Editor at the bottom of the Results table, click on the Syntax, Raw Value and/or Formatted Value columns and enter the desired value or use the drop-down list to select the desired value. The value that you enter must match the data type specified for the object. You may want to refer to the Details tab to be sure that you are entering a suitable value.  
**Note:** You can use the Table Editor to set a MIB object that MIB Tools does not include in its tree. In the Object column, enter the OID for the MIB object you want to set. (You must use the OID, not the object's text name, but you can use the last name that does exist in the tree and then add the remaining numeric OID. For example, cabletron.1.2.3.4.5.6.7.)
5. Once you have edited the values as desired, click the **Set** button. The Status Bar will display the results of the Set. (Refer to the Console event log tab for more status and error messages.)
6. Click **Query** to refresh and update the Results table with the new values.

---

**CAUTION:** Setting certain MIB objects can disable devices and cause interruptions to network operation. Do Not set MIB values unless you are sure of the outcome.

---

## Adding Rows in MIB Tables

Use the Table Editor (the bottom row of the [Results table](#)) to add rows to tables for MIBs that support this feature. You can also use these steps to remove a row from a table.

1. Be sure that you have contacted the correct device and that you have selected the [protocol](#) which provides you with write access to the desired MIB object.
2. Select the MIB table in the tree. The particular MIB table selected must support adding instances to the table. Tables that support this feature typically contain an object that shows the status of table rows and allows you to add or delete rows. For example, in the RMON MIB - **etherStatsTable**, the object *etherStatsStatus* indicates the status of the rows for that table. Select the object in the tree.
3. In the Table Editor row at the bottom of the Results table, click on the Instance column and type a value for the new instance being added to the table.
4. Click on the **Formatted Value** column and use the drop-down list to select the appropriate syntax to create a new row. This is often a string such as *createAndGo* or, as in the case of the RMON example above, *valid*. You can also click the **Raw Value** column and enter the corresponding numeric value for the syntax.  
**Tip:** When the MIB object is selected in the tree, the [Details tab](#) displays a list of valid syntax values (Formatted Value), along with the numerical code for each value (Raw Value).
5. Once you have edited values as desired, click the **Set** button. The Status Bar will display the results of the Set. (Refer to the Console event log tab for more status and error messages.)
6. Click **Query** to refresh and update the Results table. If the Set was successful, the new row will be added to the table in the device.

---

**CAUTION:** Setting certain MIB objects can disable devices and cause interruptions to network operation. Do Not set MIB values unless you are sure of the outcome.

---

## Adding MIBs to the MIB Tools Database

In order to communicate with your network devices, MIB Tools relies on a database of compiled MIB information. This database gives MIB Tools the ability

to query and set (as appropriate) any MIB object resident on your devices.

If you wish to use MIB Tools to manage devices other than Extreme Networks devices, you can add the appropriate proprietary MIBs to the MIB database. For complete instructions, see [How to Add MIBs to NetSight Console](#).

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)
- [MIB Tools Options Window](#)

## MIB Tools Overview

---

A MIB is a database maintained by the device that stores all its known management information. This information is shared between the device and remote management by means of an SNMP "agent," which retrieves information from and stores information to a MIB. When MIB information is retrieved by a remote management application (such as NetSight Console), that information is often manipulated and reorganized so that it can be displayed in a more "user-friendly" format. MIB Tools, on the other hand, provides an unadorned view of a device's MIB information, along with technical information about the MIBs themselves. It also provides the means for you to change MIB information when allowed.

Information on:

- [How a MIB is Organized](#)
- [How MIB Tools Works](#)

### *How a MIB is Organized*

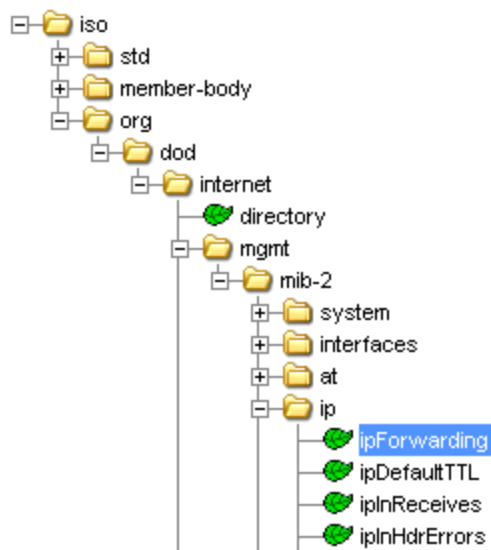
Because networking devices made by a variety of manufacturers must all be able to communicate with one another, the Internet Standards Organization (ISO) requires that each network device organize its management information according to a pre-defined "tree" format. This tree structure branches out from the ISO layer into several "sub-trees", with each sub-tree organized into "branches" (groups of related information) and "leaves" (the individual pieces of information, or objects). Among these sub-trees is an "enterprises" sub-tree, in which private vendors like Extreme Networks, can apply to the Internet

Assigned Numbers Authority for a "branch" in which to store management information (or "objects") specific to their products.

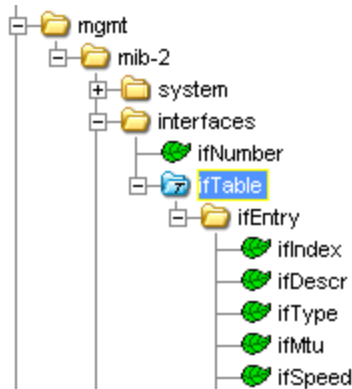
Each layer of this tree is numerically encoded, so that each branch (group) and leaf (object) is identified by a unique number known as an Object Identifier (OID). This identifier provides the path to the information stored as the Object's value, and provides the means by which the SNMP agent is able to locate the object in a device's MIB. A text name is also assigned to each branch or table OID, for convenience in identifying a management object. For example, the MIB II object *ipForwarding* is identified as follows:

- numeric OID: 1. 3. 6. 1. 2. 1. 4. 1
- ASCII string: iso /org /dod /internet /mgmt /mib-2 /ip /ipForwarding

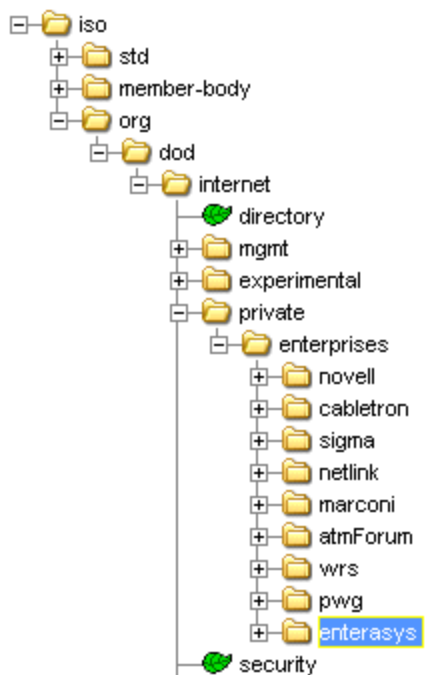
The graphic below shows how the *ipForwarding* object fits into the MIB tree. Each folder indicates that more objects are contained in that level of the tree structure. Individual objects are identified by leaf icons.



In addition, some objects may occur multiple times for a single device. Objects of this type are called "tabular objects," since they reside in tables; each occurrence of a tabular object is called an "instance," and each instance is also numerically encoded. For example, if you were querying a switch's interface table, there would be multiple instances (values) returned for each leaf object in the table (one for each port), and each instance would have a unique instance value appended to the object's OID.



Extreme Networks devices use two kinds of management information, or MIBs: standards-based MIBs such as the IETF standard MIBs, which appear under the iso > org > dod > internet > mgmt (or 1.3.6.1.2) branch of the MIB tree; and proprietary MIBs such as Extreme and Enterasys MIBs, which appear under the iso > org > dod > internet > private > enterprises (or 1.3.6.1.4.1) sub-tree.



### *How MIB Tools Works*

In order to communicate with your network devices (via SNMP), MIB Tools relies on its own database of MIB information. The OIDs, text names, and other technical information stored in this database allow you to easily search for and select the objects whose information you want to view or change. This database

gives MIB Tools the ability to query and set (as appropriate) any MIB object supported on your devices.

If you wish to use MIB Tools to manage devices other than Extreme Networks, you can add the appropriate proprietary MIBs to the MIB Tools database. See [Adding MIBs to the MIB Tools Database](#) for more information.

MIB Tools also provides the added convenience of storing a list of the devices you have contacted. This list is saved between MIB Tools sessions. (The maximum number of devices saved is specified in the [MIB Tools Options window Device tab](#).)

---

### **Related Information**

For information on related tasks:

- [How to Use MIB Tools](#)

For information on related windows:

- [MIB Tools Window](#)
- [MIB Tools Options Window](#)




## How to Verify ACLs

---

The Verify operation determines if the ACLs currently in the active configuration on your devices are the same as the ones that are defined in the ACL Manager database. You can verify the ACLs on all the devices in the ACL Manager database or only on selected devices or device groups.

### Verifying ACLs

Use the following steps to perform the Verify operation.


1. Select the device or device group in the Console left-panel tree.
2. Click the Verify button  in the right-panel ACL Manager tab.
3. If the Verify operation detects a mismatch between ACLs, the [ACL Verification Results window](#) opens where you can view the differences between the selected device's active configuration and the model in ACL Manager. The top panel lists the interfaces where there are differences between the ACLs. When an interface is selected from the top list, the lower-right panel shows the ACLs applied to the interface in the device (Device ACL) and the lower-left panel shows the ACLs for the interface that are stored in the ACL Manager database (Model ACL). Differences between the Device ACL and Model ACL are highlighted by a red exclamation mark **!**.

### Resolving Differences

If there are differences between the ACLs currently in the active configuration and the ACLs modeled in ACL Manager, use the following steps to help resolve them. Most differences can be easily resolved by choosing between the ACL in the device and the ACL in ACL Manager and then enforcing the right one on the device. But sometimes when there have been many changes, either to the ACLs in the device or to the ACLs in ACL Manager, resolving the differences may require a greater effort. To keep the process of resolving differences manageable, it is strongly recommended that you Verify ACLs frequently and make ACL Manager your primary tool for managing ACLs.

1. In the top panel of the [ACL Verification Results Window](#) select a device from the drop-down list and an interface from the table. (Only interfaces

with differences are listed.) The lower-right panel shows the ACLs applied to the interface in the device (Device ACL) and the lower-left panel shows the ACLs for the interface that are stored in the ACL Manager database (Model ACL). Differences between the Device ACL and Model ACL are highlighted by a red exclamation mark **!**.

2. Examine the differences:
  - If the rules in the Device ACL table are the ones that should be enforced for the selected target, then you must import the device ACL into the Imported ACLs folder in the ACL Editor. You can use the **Verify Devices in List** button to refresh the data in the Verification Results Window.
  - If the rules in the Model ACL table are the ones that should be enforced for the selected target, keep the Model ACL, as is. Do not import the Device ACL.
3. When you've resolved all the differences for all the targets on a particular device, **Enforce** the ACLs for that device.
  - a. Return to the ACL Manager tab and select the devices where you've just resolved the ACL differences in the Console left-panel tree.
  - b. Click the Enforce button in the ACL Manager tab .
4. Back in the ACL Verification Results Window, click **Verify Devices in List**.
5. Repeat Steps 1 through 4 until you have resolved all of the differences. If you have differences that are difficult to resolve, review the following suggestions.
  - Preserve what you have by saving your current ACL Manager database. You can now safely make changes to ACLs without concern about regression.
  - Examine the ACL in ACL Manager. Use the [ACL Packet Evaluation Tool](#) to test packets against the ACL and assess the impact of any changes before you Apply and Enforce the ACL in the device.
  - Import the ACL from the device. Use the [ACL Packet Evaluation Tool](#) to test packets against the ACL and assess the impact of any changes before you Apply and Enforce the ACL to the device.
  - If you decide to use the ACL in ACL Manager instead of the imported ACL, you must apply the Model ACL to the target before enforcing ACLs on the device.

During the verification process, if you edit or delete rules in an ACL, use the

**Verify Devices in List** button to update the Verification Results Window.

6. When you've resolved all the differences for all your devices, the Verify Results window is closed and the message " *No discrepancies were found during verify*" appears on the Status bar.
- 

## Related Information

For information on related windows:

- [ACL Verification Results Window](#)

For information on related tasks:

- [How to Enforce ACLs](#)
- [How to Manage ACLs](#)
- [How to Create ACL Rules](#)

## Working in the Left Panel

---

### Using Cut, Copy, and Paste

**Cut**, **Copy**, and **Paste** options are available from the **Edit** menu, from left-panel right-click menus, and also from buttons on the Console's main toolbar. They provide a convenient means for defining device groups in the left panel. However, not all of these options are available all the time. For example, system-created groups (blue folders) cannot be altered with these functions; so, Cut and Paste are not available from buttons or menus when any of the system-created groups are selected.

To Cut or Copy one or more objects in the tree, right click on the object and select Cut or Copy, as appropriate, from the right-click menu. You can also select an object in the tree and select Cut or Copy from the Edit menu or just click the appropriate toolbar button.

You can hold the **Shift** key and click to select consecutive objects or hold the **Control** key while clicking to select non-consecutive objects in the left panel.

### Using Drag and Drop

You can drag and drop to copy a device or device group between system-created groups or from a system-created group and a user-created group. Drag and drop functions as a *move* when dragging devices between user-created groups. Holding the Control key while dragging between user-created groups functions as a copy and paste.

To drag and drop a device or device group from one group to another:

1. Click and hold on the device or device group being copied.
2. Drag the mouse pointer over the target group and release the mouse button

---

### Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)
- [Menu Bar](#)

## How to Work with VLAN Models

---

NetSight Console lets you create VLAN models and enforce them across multiple network devices. A VLAN model consists of at least one VLAN definition and one VLAN port template, which you can define on the [VLAN Definitions window](#) and the [Port Template Definitions window](#).

**NOTE:** Configuring VLANs on an X-Pedition Router differs slightly from for other routers. Refer to [Configuring VLANs on an X-Pedition Router](#) for information that is specific to these devices.

---

Once a VLAN model has been defined, you can [verify](#) to find the differences between the definitions in the model and the VLAN settings on selected devices and their ports. You can review these differences and make modifications to your VLAN model and/or device VLAN configuration as required, including updating any or all of the definitions in the model with the settings on selected devices and their ports, and writing ([enforcing](#)) a model's VLAN definitions and/or VLAN port templates to selected devices or ports. Procedures for working with VLAN models are provided below.

Instructions on:

- [Creating a VLAN Model](#)
  - [Creating a VLAN](#)
  - [Removing a VLAN from a VLAN Model](#)
  - [Creating a Port Template](#)
  - [Removing a Port Template from a VLAN Model](#)
- [Working with VLAN Model Settings and Device VLAN Settings](#)
  - [Verifying VLANs](#)
  - [Updating VLAN Definitions from Device Settings](#)
  - [Enforcing VLANs](#)
  - [Verifying Port Templates](#)
  - [Updating a Port Template from Port Settings](#)
  - [Setting Egress States](#)
  - [Enforcing Port Settings](#)
- [Renaming Models, VLANs and Port Templates](#)

- [Editing Port VLAN Settings](#)
- [Deleting a VLAN Model](#)

## Creating a VLAN Model

NetSight Console provides you with one VLAN model (the Primary VLAN Model) which is pre-populated with a Default VLAN (VID 1). You can define this VLAN model with VLAN definitions and port templates, and/or you can create other VLAN models.

To create a VLAN model:

1. Select the **VLAN Element Editor** from the **Tools** menu.
2. In the left panel, right-click the VLAN Elements folder and select Add VLAN Model from the menu. This adds a "New VLAN Model" under the VLAN Elements folder, with its name highlighted.
3. Type a name for the newly created model, or leave the new name as is, and press **Enter**.
4. You can now create [VLANs](#) and [port templates](#) for the VLAN model.

### *Creating a VLAN*

Creating a VLAN adds a VLAN to a model's VLAN Definitions folder. It also automatically creates a port template in the same model, with the new VLAN's VID set as the PVID. NetSight Console provides you with one Default VLAN (VID 1) for the Primary VLAN Model and for any other model you create. You can define this VLAN, and/or you can create and define other VLANs.

**NOTE:** When you create multiple VLAN models, consult the **Max VLANs Supported** and **Max VLAN ID** values in the Device VLANs table of the [Device view of the VLAN tab](#), and create your VLANs based on the limitations of the device you are configuring. This will help you to avoid enforcing problems arising from conflicts between the maximums in a template and the maximums supported on a device.

To create a VLAN, follow the instructions below. To define or change a VLAN that has already been created, start with step 3.

1. Select the **VLAN Element Editor** from the **Tools** menu.
2. In the left panel, expand the VLAN Elements folder, expand the VLAN model whose VLAN(s) you want to create, then select the VLAN

Definitions folder. The [VLAN Definitions window](#) appears in the right panel.

3. Click [New](#).
4. In the VLAN Name text box in the lower portion of the Properties tab, change the name of the VLAN to fit your requirements. Do not create a VLAN name that uses any letters with diacritical marks. Diacritical marked letters are not supported by SNMP.
5. If required, change the [VID](#) for the VLAN in the VLAN ID box.
6. The VLAN retains the properties of the previously displayed VLAN. Edit these as needed (see [VLAN Definitions window](#) for more information).
7. Click **Save**. The VLAN is added to the VLAN model.
8. Once a VLAN is defined, you can compare it to ([verify](#)) the settings on selected device(s), [update](#) the model from device VLAN settings, and/or [enforce](#) the VLAN on selected devices.

Another way to create and define VLANs is to [update](#) the VLAN model with device VLAN settings, using the Device view of the [VLAN tab](#) in Console's main window.

### *Removing a VLAN from a VLAN Model*

---

- NOTES:**
1. The Default VLAN for a model cannot be deleted. If you select a Default VLAN as one of a several VLANs to be deleted, only the non-Default VLANs will be deleted.
  2. On X-Pedition Routers, If you delete a VLAN that is assigned to a port, the PVID for that port will be set to the Default VLAN (1).
- 

1. Select the **VLAN Element Editor** from the **Tools** menu.
2. In the left panel, expand the VLAN Elements folder.
3. Expand the VLAN model whose VLAN you want to remove, and expand the VLAN Definitions folder for that model.
4. In the left panel, right-click the VLAN you want to remove and select **Remove from Group**  
*or*  
in the right panel, select the VLAN in the VLANs table on the Properties tab, and click **Delete**.
5. Read the confirmation message, and click **Yes** to proceed.



## *Creating a Port Template*

When you create a new VLAN, a new port template is automatically added to the VLAN model, with the new VLAN's VID set as its PVID. You can also create your own port templates.

To create a port template, follow the steps below. To define an automatically created port template, start with step 3.

1. Select the **VLAN Element Editor** from the **Tools** menu.
2. In the left panel, expand the VLAN Elements folder, expand the VLAN model for which you want to create a port template, then select the Port Template Definitions folder. The port template [Properties tab](#) appears in the right panel.
3. Click [New](#).
4. In the Template Name text box in the lower portion of the Properties tab, change the [name](#) of the port template to fit your requirements.
5. The port template retains the properties of the previously displayed port template. Edit these as needed (see [Properties Tab \(Port Template\)](#) for more information).
6. Click **Save**. The port template is added to the VLAN model.
7. Once a port template is defined, you can compare it to ([verify](#)) the settings on selected ports, [update](#) the port template from port VLAN settings, and/or [enforce](#) the template on selected ports.

Another way to create and define port templates is to [update](#) the VLAN model with port VLAN settings, using the Advanced Port view of the [VLAN tab](#) in the Console's main window.


## *Removing a Port Template from a VLAN Model*

1. In the left panel, expand the VLAN Elements folder.
2. Select the VLAN model whose port template you want to remove, and expand the Port Template Definitions folder for that model.
3. In the left panel, right-click the port template you want to remove and select **Remove from Group**  
*or*  
in the right panel, select the port template in the upper VLAN Port Template table on the Properties tab, and click **Delete**.
4. Read the confirmation message, and click **Yes** to proceed.



## Working with VLAN Model Settings and Device VLAN Settings

You can compare (verify) a model's VLAN definitions and port templates against the settings on selected devices. You can also update the model settings from device and/or port VLAN settings, and/or enforce the VLAN definitions and/or port templates on selected devices or ports.

### *Verifying VLANs*


Verifying retrieves the VLAN settings on selected devices and compares them with the VLAN definitions in a VLAN model. Only those VLANs whose [Write VLAN to Devices](#) property is set are verified. If there are no VLAN models against which to compare the device VLAN settings, the **Start Verify (Retrieve)** button  is grayed out. For more information, see [Verifying](#).

To verify VLANs:

1. In the My Network folder on the left panel, select the device(s) or group(s) with which you wish to compare model VLAN definitions.
2. In the right panel, select the VLAN tab in Console's main window.
3. Ensure that the Device radio button is selected, and that the Device view of the [VLAN tab](#) in Console's main window is displayed.
4. Select the VLAN model whose VLAN definitions you want to verify.
5. Click **Start Verify (Retrieve)** . You can stop the verification process at any time by clicking **Stop Verify (Retrieve)** .
6. Look at the upper table. A red not-equals sign **≠** on a line indicates that there are differences between the VLAN definitions in the model and the VLAN settings on the device.
7. To view the details of the differences, select the device in the table and click **VLAN Details**. The [VLAN Details window](#) opens, where you can view the differences between the settings on the device and the VLAN definitions in the model. Click **Close** to close the VLAN Details window.
8. If you want to [update](#) VLAN definitions in your model with settings on the device(s), use the lower portion of the tab. Or, you can [enforce](#) VLAN definitions to the device(s).

## Updating VLAN Definitions from Device Settings

To update a VLAN definition with the VLAN settings on a device, use the instructions below. This operation is also called "merging."

1. In the My Network folder on the left panel, select the device(s) whose settings will be updating the VLAN definition.
2. In the right panel, select the VLAN tab in Console's main window.
3. Ensure that the Device radio button is selected, and that the Device view of the [VLAN tab](#) in Console's main window is displayed.
4. Select the VLAN model containing the VLAN definition you want to update.
5. In the VLAN Definitions for Model table in the lower portion of the tab, select the VLAN definition you want to update. You can also choose to create a new VLAN definition with the settings from the devices, by erasing the name of the VLAN definition.
6. In the right panel, select the setting(s) you want to update the VLAN definition.
7. Click **Update (Merge)** . To avoid unpredictable results, allow the merge to complete before selecting another tab or device.

---

**NOTE:** Certain devices that allow the creation of VLANs without VLAN names may create VLANs with blank names in the model. You can [rename](#) these if you like, or leave them blank. Either way, these VLANs and their properties (modified or not) will be saved when you click **Save**. However, for X-Pedition Routers, you cannot create VLANs leaving the name blank.

---

8. If you are creating a new VLAN definition, replace the generic name created by Console with a new name if desired.
9. Click **Save** to save the changes to the VLAN definition.


## Enforcing VLANs

Enforcing VLANs writes the VLAN definitions in a VLAN model to the device(s) selected in the left panel. A VLAN's [Write VLAN to Devices](#) property must be set in order for its definitions to be enforced. You may wish to [verify](#) prior to enforcing. For more information, see [Enforcing](#).


---



**NOTE:** On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS\_L3\_Interface Name). However, you can [update](#) a VLAN model definition with the System Static VLAN definition from the router.

---

1. In the My Network folder on the left panel, select the device(s) to which you want to enforce VLAN definitions.
2. In the right panel, select the VLAN tab in Console's main window.
3. Ensure that the Device radio button is selected, and that the Device view of the [VLAN tab](#) in Console's main window is displayed.
4. Select the VLAN model containing the VLAN definitions you want to enforce.
5. Click **Enforce** . To avoid unpredictable results, allow the enforce to complete before selecting another tab or device.

### *Verifying Port Templates*


Verifying retrieves the port VLAN settings on selected devices and compares them with a selected port template. The VLAN associated with the port template must have its [Write VLAN to Devices](#) property set in order for the port template to be verified. If there are no VLAN models against which to compare the port VLAN settings, the **Start Verify (Retrieve)** button  is grayed out. To verify a port template:

1. In the My Network folder on the left panel, select the device(s) with whose ports you wish to compare port templates.
2. In the right panel, select the VLAN tab in Console's main window.
3. Select Advanced Port radio button to display the Advance Port view of the [VLAN tab](#) in Console's main window displays.
4. Select the VLAN model whose port templates you want to verify.
5. Click **Start Verify (Retrieve)** . You can stop the verification process at any time by clicking **Stop Verify (Retrieve)** .
6. Look at the table. A red not-equals sign **≠** indicates that there are differences between the VLAN egress settings in the port template and the port VLAN settings on the device(s). If you select a **≠** line in the table, the port template settings are displayed. A green exclamation point **!** on that line indicates that the setting is different from the current setting on the port and will be written to the device if you enforce.

7. To view the VLAN egress settings on a port, select the port in the table and click **Egress Details**. The [VLAN Egress Details window](#) displays, where you can view the differences between the VLAN egress settings on the port and those in the port template. Click **Close** to close the VLAN Egress Details window.
8. If you want to [update](#) the port template with port VLAN settings on the device(s), use the lower portion of the tab. Or, you can [enforce](#) port templates to the device(s).

### *Updating a Port Template from Port Settings*


To update a port template with port VLAN settings from a device, follow the instructions below. This operation is also called "merging."

1. In the My Network folder on the left panel, select the device(s) whose port settings will be updating the port template.
2. In the right panel, select the VLAN tab in Console's main window.
3. Select the Advanced Port radio button to display the Advanced Port view of the [VLAN tab](#) in Console's main window.
4. Select the [VLAN Model](#) containing the port template you want to update.
5. In the left panel in the lower portion of the tab, select the port template you want to update. (If the lower portion of the tab is not showing, click the panel control up button ▲.) You can also choose to create a new port template with the settings from the ports, by erasing the name of the port template.
6. In the lower right panel, select the settings you want to update the port template.
7. Click **Update (Merge)** .
8. If you are creating a new template, replace the generic name created by Console with a new name.
9. Click **Save** to save the changes to the port template.

### *Setting Egress States*

To set the egress state for a VID prior to enforcing a port template, use the right-mouse menu in the VIDs Table on the lower right in the Port Template Properties tab. See [Egress State](#) for more information.

## Enforcing Port Settings


Enforcing writes the specified port settings to selected ports. You can enforce port settings using either the Basic Port view or the Advanced Port view of the VLAN tab in Console's main window. A green exclamation point  in a ports table indicates that the setting will be written to the device when you enforce. A VLAN's [Write VLAN to Devices](#) property must be set in order for a port template associated with it to be enforced.

### Enforcing From the Basic Port View

The Basic Port view lets you edit device port settings and enforce them, or enforce a port template (as is, or with edited settings) to selected ports. See [Editing Port VLAN Settings](#) for more information. If you wish to compare a port template to the existing VLAN settings on the ports prior to enforcing, use the [verify](#) feature in the Advanced Port view.

### Enforcing From the Advanced Port View

The [Advanced Port](#) view lets you enforce a port template to any or all ports on the devices selected in the left panel. You may wish to [verify](#) before enforcing. To enforce from the Advanced Port view of the VLAN tab in Console's main window:

1. In the My Network folder on the left panel, select the device(s) where the ports to which you want to enforce port templates are located.
2. In the right panel, select the VLAN tab in Console's main window.
3. Select the Advanced Port radio button to display the Advanced Port view of the [VLAN tab](#) in Console's main window.
4. From the [VLAN Model](#) drop-down list, select the VLAN model containing the port template you want to enforce.
5. From the [Port Template](#) drop-down list in the lower left table, select the port template you want to enforce.
6. In the upper table, select the ports to which you want to enforce.
7. Click **Enforce** . A red **X** appears if the enforcing of a particular setting fails.

## Renaming Models, VLANs, and Port Templates


To rename a VLAN model or port template:

1. In the left panel, expand the VLAN Elements folder and its subfolders until the element you want to rename displays.
2. Right-click the model or template you want to rename and select **Rename**.
3. Type the new name for the model or port template, and press **Enter**.


To rename a VLAN, follow the instructions below. You cannot rename the Default VLAN for a model.

1. In the left panel, expand the VLAN Elements folder and its subfolders until the VLAN you want to rename displays.
2. Select the VLAN.
3. In the lower left area of the Properties tab in the right panel, edit the VLAN Name text box with the new name.
4. Click **Save**.

## Editing Port VLAN Settings

You can edit the VLAN settings on individual ports using the Custom editor accessible from the **Show/Hide Table Editor** button  in the Basic Port view of the [VLAN tab](#) in Console's main window. You can either edit the existing port setting on the device, or select a port template from the drop-down list in the Custom editor and use it as is or edit it. After editing, you enforce to write the changes to the port(s).


To edit port settings:

1. In the My Network folder on the left panel, select the device(s) whose port (s) you want to edit.
2. In the right panel, select the VLAN tab in Console's main window.
3. Select the Basic Port radio button to display the Basic Port view of the [VLAN tab](#) in Console's main window.
4. Click **Show/Hide Table Editor**  to open the edit area below the table. When editing the table, refer to [VLAN Tab \(Basic Port\)](#) for column definitions, if needed.
  - *To change an existing setting on the port:* Select the port you want to edit. In the Table Editor, edit the appropriate column, pressing **Enter** after editing each column.

- *To use settings from a port template to edit port settings:* Select the port(s) you want to edit. Select the VLAN model at the top of the tab, then select the port template from the **Custom** drop-down list. (When you select a template, the column values change to the template settings, but the choice in the drop-down box still displays **Custom**.) You can leave the template settings as is, or use the Table Editor to edit them as needed. Settings not checked in the template itself are not editable (see [Port Template Definitions](#) view. Press **Enter** after editing a column.

**NOTE:** GVRP, GARP Join Time, GARP Leave Time, GARP Leave All Time, and Configure Egress States are not set in the Basic Port view. Use the Advanced Port View to set these values.

5. A green exclamation point  appears in the table if a setting will be written to the port when you enforce.
- 

**NOTE:** To cancel changes and restore the original values, click  to hide the Table Editor before enforcing the values in the table.

---

6. Click **Enforce** . A red **X** appears if the enforcing of a particular setting fails.

## Deleting a VLAN Model

To delete a VLAN model:

1. In the left panel, expand the VLAN Elements Editor.
  2. Right-click the VLAN Model you want to delete and select **Remove from Group**. Read the confirmation message, and click **Yes** to proceed.
- 

### Related Information

For information on related concepts:

- [VLAN Concepts](#)

For information on related tasks:

- [Configuring VLANs on an X-Pedition Router](#)

For information on related windows:



- [Port Template Definitions](#)
- [VLAN Definitions](#)
- [VLAN Tab \(Advanced Port\)](#)
- [VLAN Tab \(Basic Port\)](#)
- [VLAN Tab \(Device\)](#)

---

## Configuring VLANs on an X-Pedition Router

---


Because X-Pedition routers perform some self configuration, setting up VLANs on these devices with Console may occasionally be confusing. Thorough planning for the VLANs on your network and this topic can help you to configure VLANs on your X-Pedition routers.

### *Creating VLANs on X-Pedition Routers*

Here is the recommended outline for establishing VLANs on your X-Pedition routers:

- Create a separate VLAN Model for your X-Pedition routers.
- Decide what VLANs you'll need on your network and create as many VLAN Definitions for each.
- Synchronize the VLANs on your X-Pedition devices with the VLANs that you've created in Console.
- Make changes to your VLAN Definitions as necessary and Enforce.
- Decide which ports will be used as trunk ports and which will be used as access ports (these are determined by your settings for the Acceptable Frame Type on the various ports) and create Port Template Definitions for those ports.
- Add the ports to the desired VLANs egress lists, assign PVIDs and apply Port Templates to selected ports.
- Enforce.
- Make changes to VLANs, Port Templates, and PVIDs as necessary and Enforce.

**1. Create a VLAN model dedicated to X-Pedition routers:**

- a. Click the VLAN tab in the right panel of the Console main window.
- b. Select the **VLAN Element Editor** from the **Tools** menu (or click the  on the toolbar).
- c. In the left panel of the VLAN Element Editor, right-click the VLAN Elements folder and select Add VLAN Model from the popup menu. This adds a "New VLAN Model" under the VLAN Elements folder, with its name highlighted.
- d. Type a name for the newly created model, or leave the new name as is, and press **Enter**.

**2. Create your VLANs:**

- a. In the left panel, expand the VLAN Elements folder, expand your new VLAN model, then select the VLAN Definitions folder. The [VLAN Definitions view](#) appears in the right panel.
- b. Click **New**.
- c. In the VLAN Name text box in the lower portion of the VLAN Definitions view, change the name of the VLAN to fit your requirements. Although the VLAN name is only serves as a human-readable element, you cannot create a VLAN on an X-Pedition router if its name is left blank.
- d. If required, change the [VID](#) for the VLAN in the VLAN ID box.
- e. Define the properties for your new VLAN. The VLAN retains the properties of the previously displayed VLAN. Edit these as needed.
  - Check **Write VLAN to Devices**. This will download this VLAN Definition to selected devices when you enforce.
  - Uncheck **Dynamic Egress** and **IGMP**. Dynamic Egress and IGMP are not supported on X-Pedition Routers.
  - If you are creating this VLAN using an **X-Pedition Protocol Filter**, check X-Pedition Protocol Filter and select a protocol from the Protocols area.

---

**RECOMMENDATION:** Create a separate VLAN for each protocol filter that you will be configuring. Do not create more than one VLAN using the same protocol filter.



---

- 
- NOTES:**
1. You cannot change and enforce the X-Pedition Protocol Filters for the Default VLAN.
  2. If this VLAN will be assigned to an access port (Acceptable Frame Type set to Accept All), then you can only select a single protocol and that protocol cannot be configured for another VLAN.
- 


- f. Click **Save**. The VLAN is added to the VLAN model.
- g. Repeat these steps to create additional VLANs.

X-Pedition routers are configured with System Static VLANs that cannot be changed. These System Static VLANs should be merged with your new VLAN Definitions to synchronize the VLAN definition on your devices with the definitions in Console.

### 3. Synchronize VLAN Definitions:

- a. In left panel of Console's main window, select the devices where you want to apply your new VLANs.
- b. In the right panel, select the **VLAN** tab and click **Device**.
- c. Select the Static System VLANs (VLAN names begin that with SYS-- e.g., SYS-L3-SmartTrunk-Only-Intf) in the **VLAN Definitions for Device: x.x.x.x** table.
- d. Select any other VLANs on the device that you want to include in your VLAN definition. If you are not sure, merge them now. You'll be able to delete then later or change them and enforce them with your changes.
- e. Click  Merge to add the VLANs from the device into your VLAN model.
- f. In the VLAN Elements Editor, VLAN Definitions folder.
- g. Select each VLAN merged from the device, in turn, and delete unwanted VLANs and change definitions where necessary. Refer to [Modifying VLANs](#) for information on changing VLAN Definitions, then return here to enforce your VLANs.
- h. When you're satisfied with the definitions, click  to enforce your VLAN definitions in the VLAN tab, Device view.

---

**NOTE:** X-Pedition devices do not always refresh the tables and views in Console when you perform an enforce. So, you must click  Retrieve, after an enforce to see the correct results in Console's views.

---

#### 4. Define your Port Templates:

- a. Select the Port Templates folder in the left panel of the VLAN Elements Editor window.
- b. Click **New** to add a new Port Template.
- c. In the Port Template Name field, change the name of the Port Template to fit your requirements.
- d. If you know the particular VLAN ID that you will be assigning with this Port Template, check **Set PVID** and select the VLAN ID from the associated drop-down list. Otherwise leave **Set PVID** unchecked. You will be able to assign the PVID later when you assign VLANs to selected ports.
- e. Uncheck **Ingress Filtering**, **GARP Join Time**, **GARP Leave Time**, and **GARP Leave All Time**. These features are not supported in the X-Pedition.
- f. If you are configuring this template for a trunk port, click **Acceptable Frame Type** and select **Accept Tagged Only** from the drop down list. The PVID Egress State is automatically updated to **Tagged**.
- g. If you are configuring this template for an access port, click **Acceptable Frame Type** and select **Accept All** from the drop down list. The PVID Egress State is automatically updated to **Tagged**.

- 
- NOTES:**
1. If this Port Template specifies a VLAN that will be assigned to an access port (Acceptable Frame Type set to Accept All), then the VLAN can only specify a single protocol for the X-Pedition Protocol Filter and that protocol cannot be configured for another VLAN.
  2. You can also create Port Templates to define other common port configurations and apply them from either the VLAN tab Basic or VLAN tab Advanced view.
- 

- h. Always check **Configure Egress States**. Do not click **Make Q Trunk**
- i. Set the **Egress State** for all the System Static VLANs in the table to **No Change**. (Select all of the System Static VLANs, then right click on one

and choose **No Change** from the popup menu.)

j. Click **Save**.






#### 5. Assign Port Templates to your device ports.

This can be done from either the VLAN tab, Basic or Advanced view. The following steps show you how to assign Port Templates using the VLAN tab, Advanced view:




- a. Click a FlexView Tab (e.g., Interface Summary) and open the 802.1Q VLAN Static Table FlexView. (click  Open and navigate into the VLAN folder, then select 802.1Q VLAN Static Table.tpl.)

**NOTES:** In an X-Pedition Router:

1. You cannot assign a VLAN to a port unless the VLAN exists on the device. You must first enforce the VLAN from the VLAN tab, Device view.
2. You cannot assign a VLAN to a port (set the PVID) unless the port is listed on the VLANs Egress list. The 802.1Q VLAN Static Table FlexView is where you can add ports to a VLAN's Egress list.

6. Select the device(s) where you want to assign PVIDs or Port Templates and click  Retrieve on the FlexView toolbar.
7. Click , select the VLAN that you want to apply to a port and type the port number(s) into the table editor row for the **Static Egress Ports** column.
8. Repeat step c to assign other VLANs to other ports.
9. Click  Enforce.
10. Click the VLAN tab **Advanced** view in the Console main window.
11. In the table in the upper half of the view, select the port(s) where you want to assign a Port Template (one or more of the ports added to the VLANs Static Egress Ports list in step c).
12. Select a port template from the Port Template drop-down list in the lower right side of the view.
13. Click  Enforce and then  Retrieve. If you checked **Set PVID** and defined a particular VLAN ID when you created your Port Template, then the PVID for the ports has been set to the VLAN ID that you specified. If you left **Set PVID** unchecked, you must now assign a VLAN (set the PVID) on those ports.

#### 14. Assign VLANS to your device ports:

- a. Click the VLAN tab, **Basic** view in Console's main view and click .
- b. Select a port where you want to assign a VLAN (one of the ports added to the VLANs Static Egress Ports list in step 5c).
- c. Click the table editor row for the PVID column and select a VLAN ID from the drop-down list.
- d. Repeat steps b and c to assign additional VLANs to other ports.
- e. Click  Enforce and then  Retrieve. The PVID on the selected ports is now set to the selected VLAN ID.

**NOTE:** On the X-Pedition Router, assigning a PVID (that exists on the device) in the Basic Port view and enforcing may incorrectly report an error, placing a red **X** in the PVID table cell.

Refresh the table by performing a **Retrieve** to remove the **X**.

### *Modifying VLANs on X-Pedition Routers*

This section provides help for tasks that may differ slightly for X-Pedition Routers from how the same task is performed for other routers.

Instructions on:

- [Removing a VLAN from a VLAN Model](#)
- [Editing Port VLAN Settings](#)
- [Deleting a VLAN Model](#)


#### Removing a VLAN from a VLAN Model

- NOTES:**
1. The Default VLAN for a model cannot be deleted. If you select a Default VLAN as one of a several VLANs to be deleted, only the non-Default VLANs will be deleted.
  2. On X-Pedition Routers, If you delete a VLAN that is assigned to one or more ports, the PVID for those ports will be set to the Default VLAN (1).


1. Select the **VLAN Element Editor** from the **Tools** menu.
2. In the left panel, expand the VLAN Elements folder.
3. Expand the VLAN model whose VLAN you want to remove, and expand the VLAN Definitions folder for that model.

4. In the left panel, right-click the VLAN you want to remove and select **Remove from Group**  
*or*  
in the right panel, select the VLAN in the VLANs table on the Properties tab, and click **Delete**.
5. Read the confirmation message, and click **Yes** to proceed.

## Editing Port VLAN Settings


You can edit the VLAN settings on individual ports using the Custom editor accessible from the **Show/Hide Table Editor** button  in the Basic Port view of the [VLAN tab](#) in Console's main window. You can either edit the existing port setting on the device, or select a port template from the drop-down list in the Custom editor and use it as is or edit it. After editing, you enforce to write the changes to the port(s).

To edit port settings:

1. In the My Network folder on the left panel, select the device(s) whose port (s) you want to edit.
2. In the right panel, select the VLAN tab in Console's main window.
3. Select the Basic Port radio button to display the Basic Port view of the [VLAN tab](#) in Console's main window.
4. Click **Show/Hide Table Editor**  to open the edit area below the table. When editing the table, refer to [VLAN Tab \(Basic Port\)](#) for column definitions, if needed.
  - *To change an existing setting on the port:* Select the port you want to edit. In the Table Editor, edit the appropriate column, pressing **Enter** after editing each column.
  - *To use settings from a port template to edit port settings:* Select the port(s) you want to edit. Select the VLAN model at the top of the tab, then select the port template from the **Custom** drop-down list. (When you select a template, the column values change to the template settings, but the choice in the drop-down box still displays **Custom**.) You can leave the template settings as is, or use the Table Editor to edit them as needed. Settings not checked in the template itself are not editable (see [Port Template Definitions](#) view. Press **Enter** after editing a column.

- NOTES:**
1. If you change the Acceptable Frame Type to Accept Tagged Only, the port becomes a trunk port and the PVID is automatically set to the Default VLAN.
  2. Configure Egress States cannot be set in the Basic Port view. Use the Advanced Port View to set these values.
  3. GVRP, GARP Join Time, GARP Leave Time, GARP Leave All Time, are not supported in the X-Pedition Router.
- 

5. A green exclamation point  appears in the table if a setting will be written to the port when you enforce.
- 

**NOTE:** To cancel changes and restore the original values, click  to hide the Table Editor before enforcing the values in the table.

---

6. Click **Enforce** . A red **X** appears if the enforcing of a particular setting fails.

**NOTE:** On the X-Pedition Router, assigning a PVID (that exists on the device) in the Basic Port view and enforcing may incorrectly report an error, placing a red **X** in the PVID table cell.

Refresh the table by performing a **Retrieve** to remove the **X**.

## Deleting a VLAN Model

To delete a VLAN model:

1. In the left panel, expand the VLAN Elements Editor.
  2. Right-click the VLAN Model you want to delete and select **Remove from Group**. Read the confirmation message, and click **Yes** to proceed.
- 

- NOTES:**
1. The Default VLAN for a model cannot be deleted. If you select a Default VLAN as one of a several VLANs to be deleted, only the non-Default VLANs will be deleted.
  2. On X-Pedition Routers, If you delete a VLAN that is assigned to one or more ports, the PVID for those ports will be set to the Default VLAN (1).
- 
- 

## Related Information

For information on related concepts:

- [VLAN Concepts](#)



For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

- [Port Template Definitions](#)
- [VLAN Definitions](#)
- [VLAN Tab \(Advanced Port\)](#)
- [VLAN Tab \(Basic Port\)](#)
- [VLAN Tab \(Device\)](#)

# Extreme Management Center Console Windows

---

The **Windows** section contains Help topics describing Extreme Management Center Console windows and their field definitions.

## ACL Editor

---

Use the ACL Editor to create a new ACL or modify an existing ACL. The ACL Editor is divided into a left panel and a right panel. The left panel displays a hierarchical representation of your ACLs and their rules. The tabbed pages in the right panel display detailed information about the item selected in the left-panel tree.

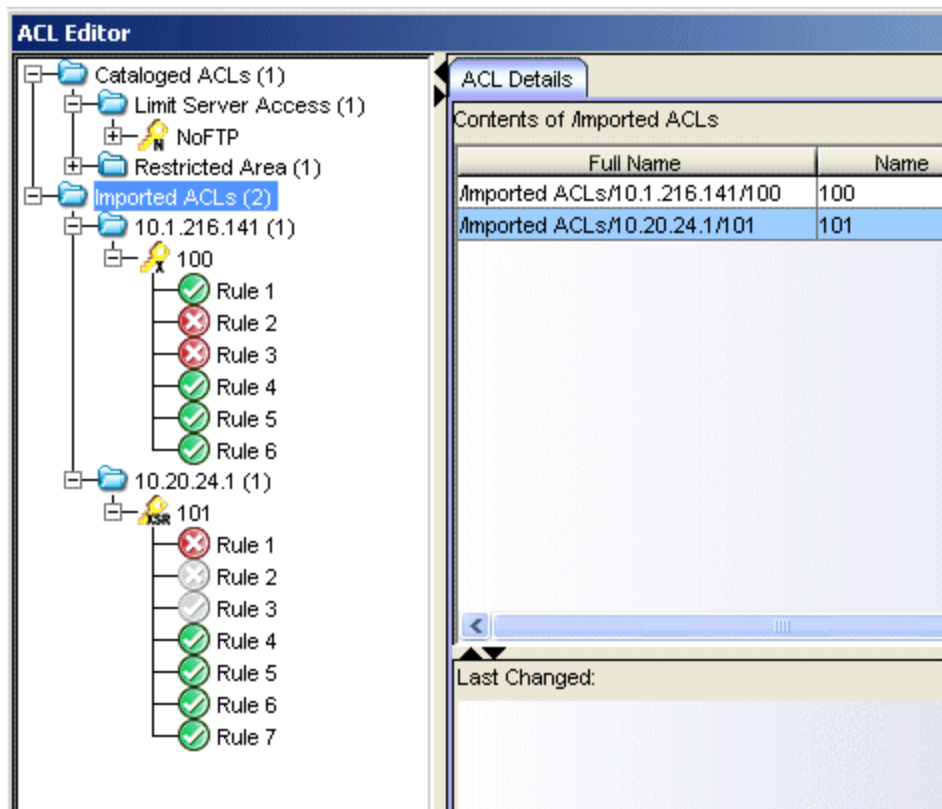
To access the ACL Editor, click the  button in the ACL Manager tab.

Information on:

- [Left-Panel Tree](#)
- [ACL Details Tab](#)
- [Editor Tab](#)
- [Description Tab](#)
- [Targets Tab](#)
- [CLI Preview Tab](#)

### Left-Panel Tree

The left-panel tree in the ACL Editor displays all your Cataloged and Imported ACLs and their rules.



### Cataloged ACLs Folder

The Cataloged ACLs folder contains all ACL folders, ACLs, and rules that have been either created using the ACL Editor or moved from the Imported ACLs folder.

### Imported ACLs Folder

The Imported ACLs Folder contains ACLs that have been imported from a file or from network devices and have not yet been documented and moved to the Cataloged ACLs Folder.

### ACLs

ACL Manager supports five types of ACLs: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. The type of ACL is indicated on the ACL icon. The S/K/N 7.x+ ACL displays a icon and the N-Series 6.x displays a icon.

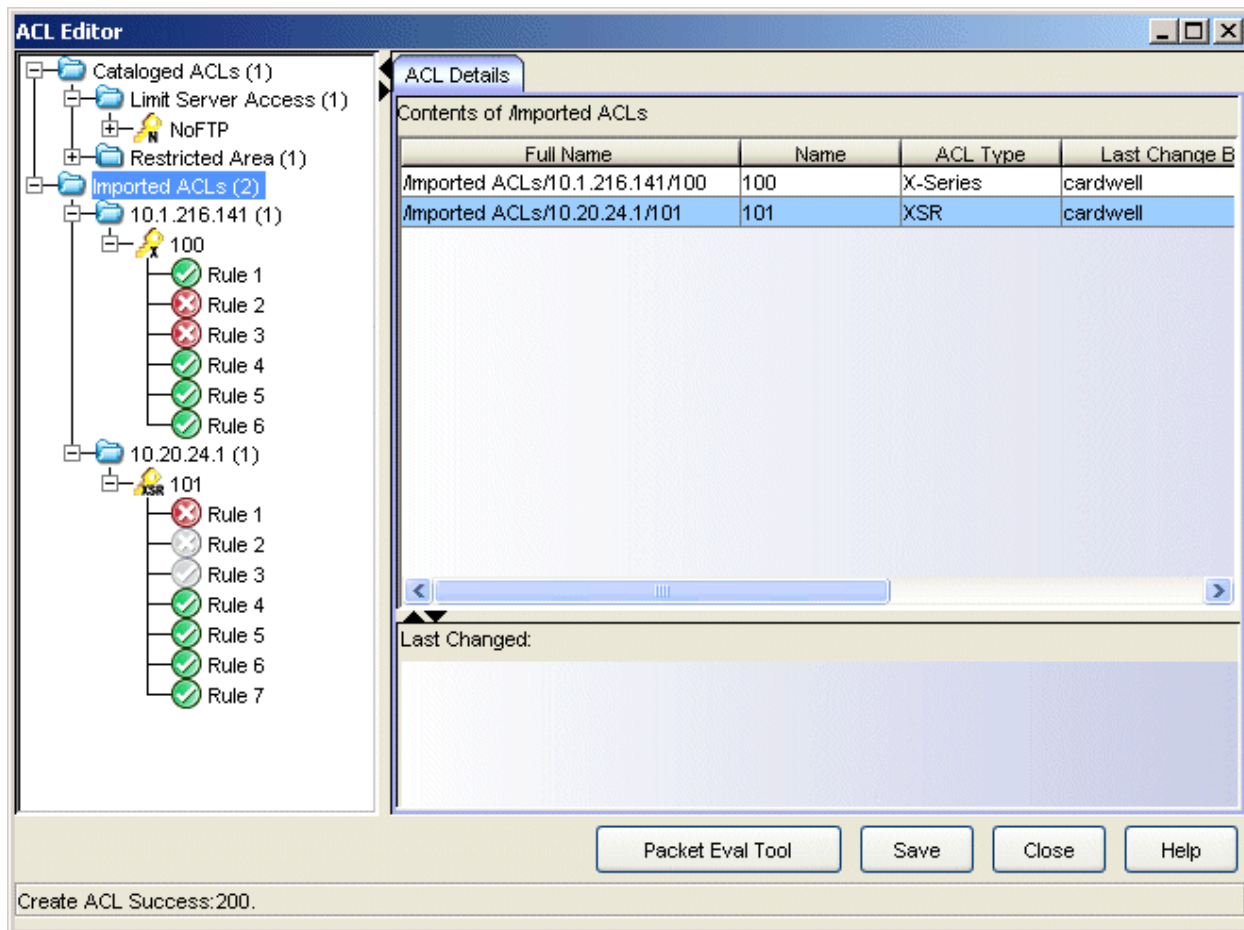
### Rules

Rules provide specific access definitions within an ACL. The following icons let you differentiate between rules with permit and deny actions. Rule icons that have been commented (disabled) appear grayed-out.

- Permit Rule     Commented Permit Rule
- Deny Rule     Commented Deny Rule

## ACL Details Tab

The ACL Details tab presents a list of all the ACLs contained within the folder selected in the left-panel tree.



### Full Name

The full path to the ACL's location in the ACL Editor tree.

### Name

The ACL name.

### ACL Type

The ACL type: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. This identifies the command line syntax of the ACL.

### Last Change By

Identifies the user that made the most recent change to this ACL data. This field is updated when the device data is imported or refreshed and there have been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Change By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

### Last Change Date

Gives the date and time of the most recent change to this ACL. This field is updated when the device data is imported or refreshed and there have been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Change Date" field is updated when the database data is updated, not when the device is modified, such as during an enforce.


### Description

A description of the selected ACL. This is the description entered in the right-panel [Description tab](#) when an ACL is selected.

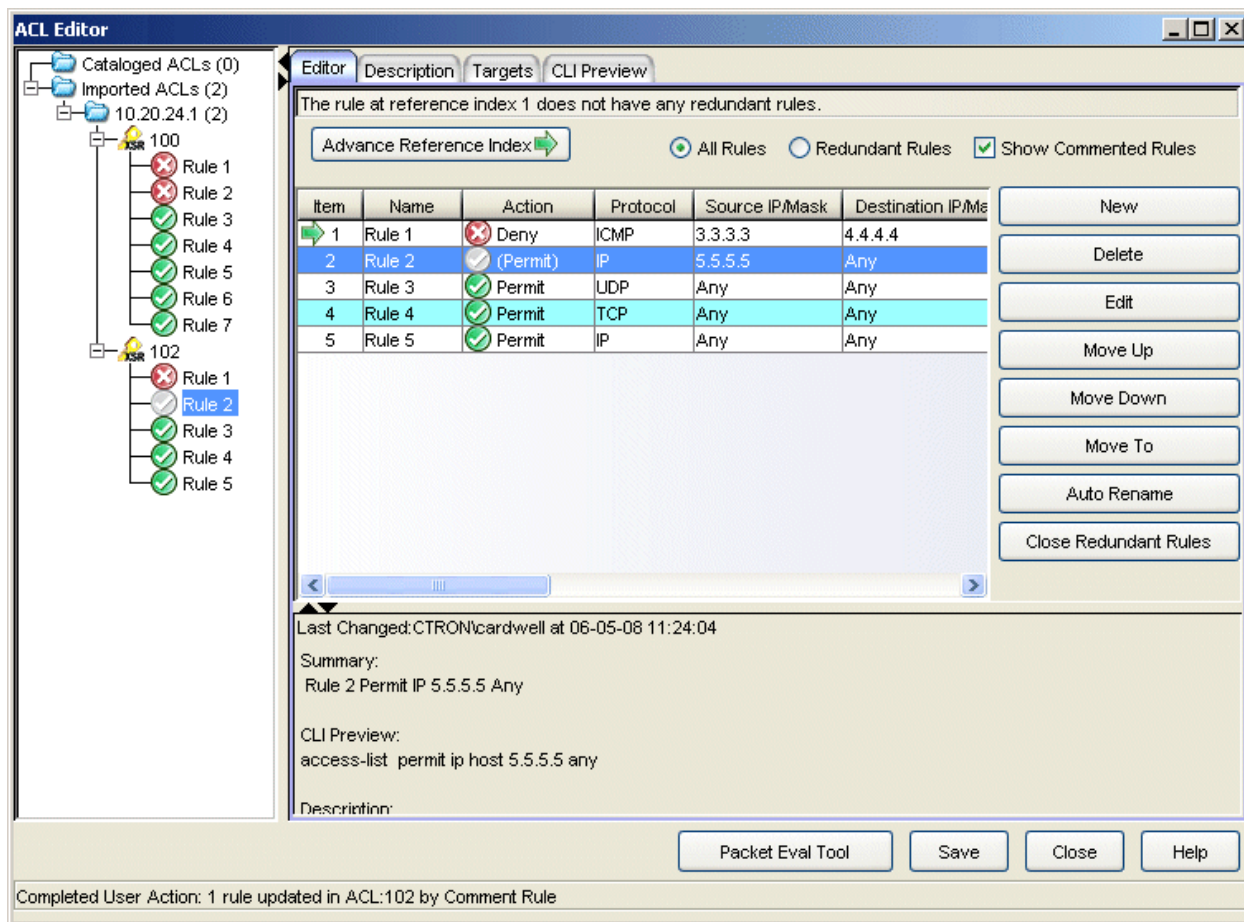
## Editor Tab

The Editor tab presents a table that lists the rules contained within the selected ACL and lets you create, edit, and modify the rules. You can use the radio buttons at the top of the tab to select whether to display all rule contained within the ACL, or only those rules that are involved in redundancies. Rules are considered redundant if, with the exception of their Action and Logging settings:

- they are the same rule type (when searching for redundant rules, UDP and TCP rules are treated as IP rule types when they follow an IP rule, because UDP and TCP are subsets of IP) and
- both rules are defined by parameters that would match the same packet traffic. A more specific rule is considered redundant when it follows a more generally defined rule in the ACL. For example, a rule that defines a specific IP address as the Source Address will be considered redundant if it follows a rule that defines the Source Address as Any.

The green Reference Index arrow  determines the rule that is being compared. ACL Manager compares this rule with all the remaining rules in the ACL. When a redundant rule is detected, it is marked with a red exclamation mark (!). Use the radio buttons to determine whether the list will display all of the rules in the

selected ACL or only rules involved in redundancies. Select the Show Commented Rules checkbox if you would like to display rules that are commented out. The Advance Reference Index button lets you advance the Reference Index arrow to the next rule to compare. Buttons on the right side of the tab let you auto rename, edit, and rearrange rules in the list.



### Item

Reference number for the rules in the selected ACL.

### Name

The names of the rules in the selected ACL.



### Action

The rule's action: Permit, Deny, or Remark. The rule action determines how packets that match the rule's parameters will be handled.






Permit allows access when the packet matches the protocol and parameters defined for this rule.

---

	Deny discards the packet if it matches the protocol and parameters defined for this rule.
	Remark is used as a way to add a remark to the ACL (K-Series, S-Series, and N-Series with 7.x firmware only)

---

Commented rules appear as a gray icon, either permit () or deny () or remark ().

---

### Protocol

The type of protocol to which this rule is applied.

### Source IP Mask

This column contains a source address to be compared against the source address of an incoming packet. This can be **Any** source address, a specific IP address, or subnet address. **Any** is a wildcard statement that automatically matches the source address in a packet's header.

### Destination IP Mask

This column contains a destination address to be compared against the destination address of an incoming packet. This can be **Any** destination address or a specific IP address. **Any** is a wildcard statement that automatically matches the destination address in a packet's header.

### Src Port

This column contains a source port to be compared against the source port of an incoming packet. This can be **Any** source port or a specific port address. **Any** is a wildcard statement that automatically matches the source port in a packet's header.

### Dest Port

This column contains a destination port to be compared against the destination port of an incoming packet. This can be **Any** destination port or a specific port address. **Any** is a wildcard statement that automatically matches the destination port in a packet's header.

### TOS

The ToS (Type of Service) value configured for the rule. The rule will allow or reject traffic based on the TOS value specified here.

### Precedence

The Precedence value configured for the rule. The rule will allow or reject traffic based on the Precedence value specified here.



**DSCP**

The DSCP (Diffserv Codepoint) value configured for the rule. The rule will allow or reject traffic based on the DSCP value specified here.

**IP Protocol Num**

The IP Protocol Number configured for the rule. The rule will allow or reject traffic based on the IP Protocol Number value specified here.

**Message Type**

Message type for the rule. ICMP rules can be defined to allow or reject traffic based on ICMP Message Type (0 to 255).

**Message Code**

Message code for the rule. ICMP Rules can be defined to allow or reject traffic based on ICMP Message type. When a Message Type is specified, an optional ICMP Message Code (1 to 255) can be used to create a more specific rule.

**Established**

Indicates whether this rule will allow TCP/UDP responses through the router, provided the connection between two hosts is already established: true or false.

**Logging**

Indicates whether logging is enabled for this ACL: true or false. When enabled, a Log message is sent to the console and if you have a Syslog server configured, the same message is sent to the Syslog server.

**Last Change**

Indicates the date and time that the device's ACL data in the database was last changed, and the user that initiated the action. This field is updated when the device data is imported or refreshed and there have been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

**Notes**

A description of the rule. Notes can be added when you create or edit a rule.

**New Button**

Opens the [Add to ACL window](#) where you can create a new rule to add to the selected ACL.

**Delete Button**

Deletes the selected rule or rules.

**Edit Button**

Opens the [Edit ACL window](#) where you can edit the selected rule.

**Move Up/Move Down Buttons**

Re-positions the selected rule up or down in the ACL. Each click moves the rule one row.

**Move To Button**

Moves the selected rule to the line number entered into the associated field.

**Auto Rename Button**

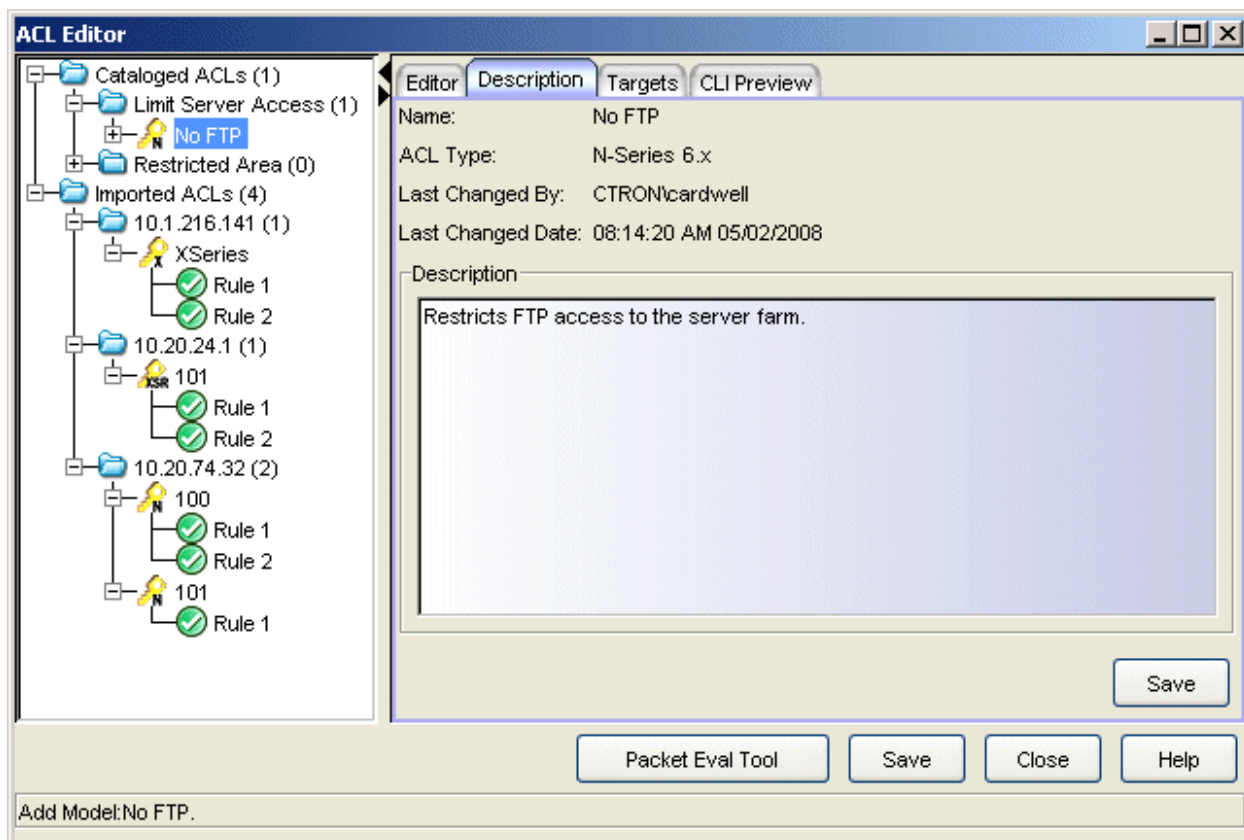
Renames (re-numbers) rules that were created using the default name (Rule1, Rule2, etc.) to correspond to the index numbering.

**Close Redundant Rules Button**

Closes the top section of the tab and removes any redundant rule indicators.

## Description Tab

The Description tab provides a text box where you can enter a description for the selected ACL and keep a record of changes made to the ACL.

Sample Description Tab**Name**

The ACL name.

**ACL Type**

The ACL type: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. This identifies the command line syntax of the ACL.

**Last Changed By**

Identifies the user that made the most recent change to this ACL data. This field is updated when the device data is imported or refreshed and there have been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

**Last Changed Date**

Gives the date and time of the most recent change to this ACL. This field is updated when the device data is imported or refreshed and there have

been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Changed Date" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

## Description

An area where you can enter text to describe the purpose for the selected ACL.

## Targets Tab

The Targets tab lists specific details about where the selected ACL is applied.

The screenshot shows the ACL Editor application window. The left pane displays a tree view of ACLs under 'Imported ACLs (4)'. The selected ACL is '100' under '10.20.74.32 (2)'. The main pane shows the 'Targets' tab with a table listing the applied targets.

Device	Target Type	Target	Direction	Logging	Applied By	Applied
10.20.74.32	Interface	Vlan 111	Inbound	N/A	CTRON\card...	03/25
10.20.74.32	Interface	Vlan 113	Outbound	N/A	CTRON\card...	03/25

Completed User Action: 1 rule updated in ACL:101 by Delete Rule

## Device

Identifies the device where the selected ACL is currently applied.

## Target Type

Target Type can be an agent service (SNMP, Telnet HTTP, or SSH) or logical interface to which this ACL is applied.

## Target

The name of the agent service or interface where this ACL is currently applied.

**Direction**

Identifies the traffic direction (Inbound or Outbound) for which this ACL is applied.

**Logging**

Indicates whether logging is enabled or disabled for this ACL.

**Applied By**

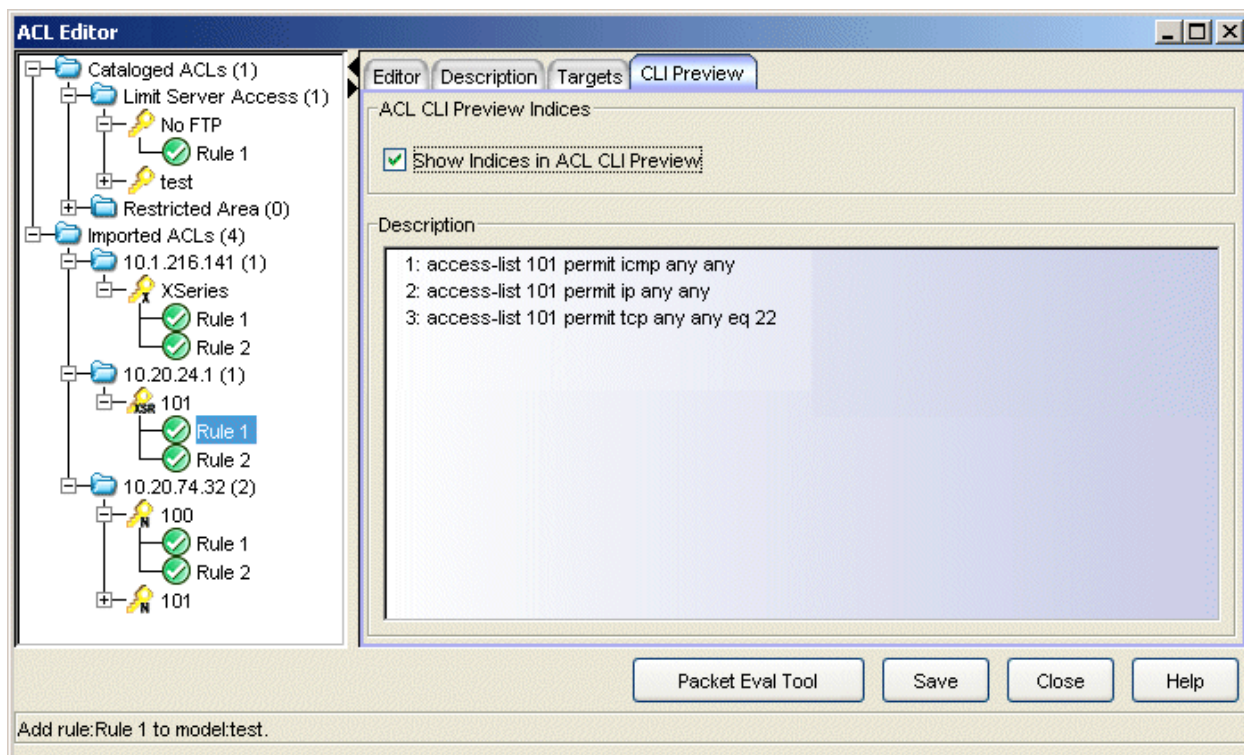
Identifies the user that applied this ACL.

**Applied Date/Time**

Indicates the date and time when the ACL was applied.

**CLI Preview Tab**

This tab shows the rules that you've defined in K-Series, S-Series, N-Series, X-Series, or XSR CLI syntax, according to the ACL type. When a Common ACL is selected from the left panel, the rule is displayed as a generic Common-type rule. Rules that are commented do not appear in the CLI Preview. You can enable/disable line numbering using the **Show Indices in ACL CLI Preview** checkbox.

**Sample CLI Preview Tab**

**Packet Eval Tool Button**

Opens the [Packet Evaluation Tool](#) that lets you verify the intended action of the ACLs selected in the left-panel tree.

**Save Button**

Saves any changes you have made in the ACL Editor to the ACL Manager database.

---

**Related Information**

For information on related windows:

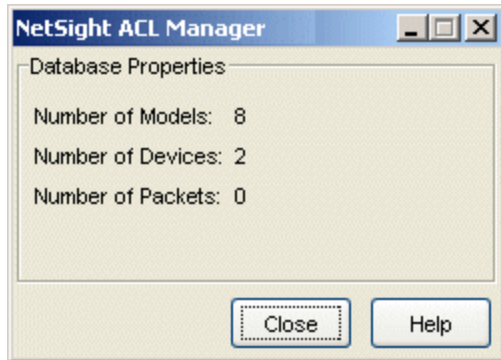
- [Add to ACL Window](#)

# ACL Manager

## Database Properties Window

---

The ACL Manager Database Properties window displays information about the database contents.



### Number of Models

The number of unique ACL objects defined in the ACL Manager database.

### Number of Devices

The number of devices that have ACL information imported into the ACL Manager database.

### Number of Packets

The number of test packets saved for the Packet Evaluation tool.

---

## Related Information

For information on related windows:

- [ACL Manager Tab](#)

## ACL Packet Evaluation Tool

---

This tool lets you verify the intended action of an ACL. You can use the tool to define a packet and then evaluate whether it would be permitted or denied by an ACL. Test results are presented in the [Editor tab](#), showing which rules allowed or denied the test packet.

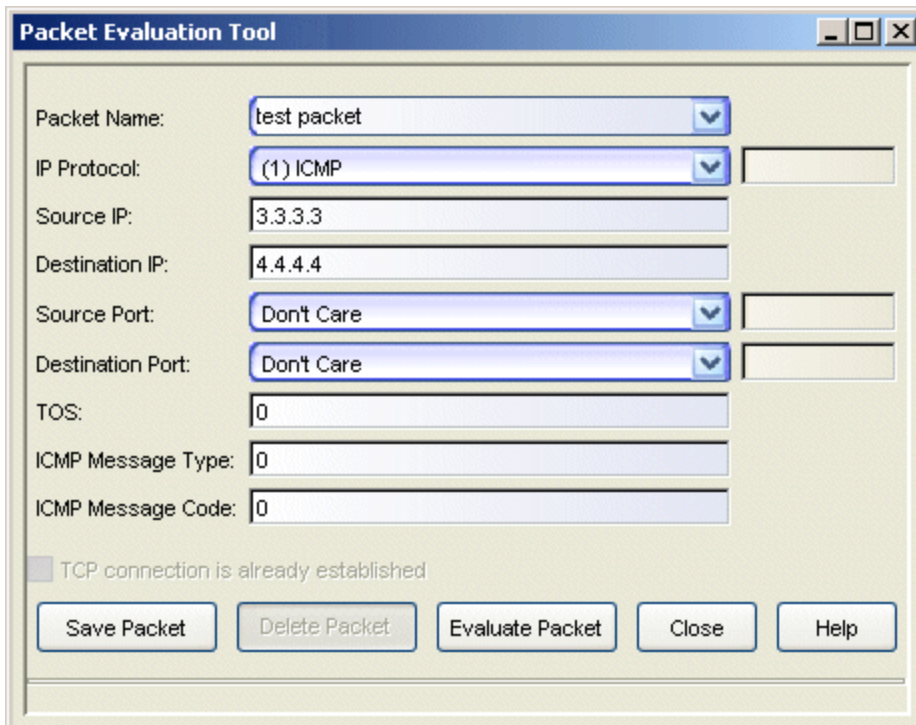
---

**CAUTION:** This tool only tests whether or not a defined packet will be denied or allowed based on the ACLs selected for the test. This tool will not verify that the packet will actually hit the selected ACLs based on other router configurations.

---

Use the following steps to use the Packet Evaluation Tool.

1. Open the ACL Editor and select the ACL that you want to test in the left-panel tree.
2. Click the **Packet Eval Tool** button at the bottom of the ACL Editor window. The ACL Packet Evaluation Tool opens.



The screenshot shows the "Packet Evaluation Tool" dialog box. It contains the following fields and controls:

- Packet Name: test packet (dropdown menu)
- IP Protocol: (1) ICMP (dropdown menu)
- Source IP: 3.3.3.3 (text input)
- Destination IP: 4.4.4.4 (text input)
- Source Port: Don't Care (dropdown menu)
- Destination Port: Don't Care (dropdown menu)
- TOS: 0 (text input)
- ICMP Message Type: 0 (text input)
- ICMP Message Code: 0 (text input)
- TCP connection is already established
- Buttons: Save Packet, Delete Packet, Evaluate Packet, Close, Help



3. Use the **Packet Name** drop-down list to select a previously defined packet to use with this test, or enter a new packet name. If you select a previously defined packet, you can use the packet as defined or modify parameters as needed for the current test. You do not need to enter a name if you will not be saving the packet.
4. Use the **IP Protocol** drop-down list to select the protocol for this test packet. You can select a pre-defined well-known ID or select Other and enter a number.
5. Enter the source IP address for this packet.
6. Enter the destination IP address for this packet.
7. Use the **Source/Destination Port** drop-down lists to specify the source/destination protocol port as one of the following values:
  - **Don't Care** - bypass matching the source/destination port to the source/destination in the ACL rules, effectively matching any source/destination.
  - A pre-defined well-known TCP/UDP port.
  - **Other** - Select this value and then specify a port number (1 through 65535).
8. Enter a TOS (Type of Service) value. TOS defines the one-byte TOS, IPv4 or IPv6 DS (Differentiated Service) field contained in the IP header of a frame for the test packet. The TOS can be set to a specific decimal number between 0 and 255.

**NOTE:** IPv4 defines this field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.
9. If ICMP is the selected IP Protocol type, a **Message Type** can be defined to allow or reject traffic based on the ICMP Message Type value. ICMPv6 message types 0 to 127 are with error messages and informational messages have message types from 128 to 255. When a Message Type is specified, an optional ICMP **Message Code** (0 to 255) can be used to create a more specific rule.
10. The **TCP connection** check box is only enabled if (6) TCP is selected as the IP Protocol type. Select this checkbox if the packet being tested is supposed to be part of a TCP session that is already established.

11. Click **Save Packet** to save this test packet for future testing. A name must be assigned to the packet before it can be saved.
12. Click **Evaluate Packet** to perform the ACL test.

Test results showing which rules allowed or denied the test packet are presented in the Editor tab of the ACL Editor. The particular rules that match the defined packet are noted by a green arrow in the left column. When multiple rules apply, all are noted with an arrow. However, the first rule that matches in the list is the rule that determines whether the packet is forwarded or dropped.

When you have finished using the Packet Evaluation Tool, close the window and then use the **Close Evaluate Rules** button in the right-panel of the ACL Editor to remove the green arrows from the Editor tab.

---

### Related Information

For information on related windows:

- [ACL Editor](#)
- [Add to ACL Window](#)

For information on related tasks:

- [How to Create ACL Rules](#)

## Pre-Defined Well-Known IDs Window ACL Manager

---

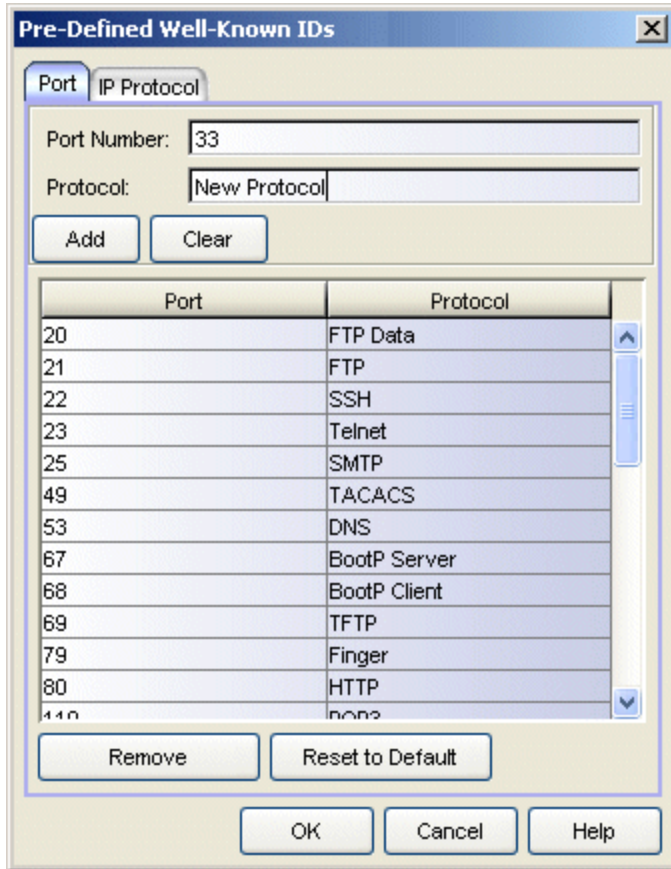
This window lets you add to the pre-defined list of well-known identifiers (IDs) used when creating certain ACL rules. You can define a new ID for a TCP/UDP port number or for an IP-Protocol type. Once defined, these IDs are available for selection from the list of well-known values when creating TCP, UDP, or IP-Protocol rules.

To access the window, right-click the menu button at the top of the ACL Manager tab and select **Well Knowns**. IDs are defined using either of two tabs:

- [Port Tab](#)
- [IP Protocol Tab](#)

### Port Tab

The Port tab lets you define a new ID for a TCP/UDP port number. Once defined, this ID can be used when creating a TCP or UDP rule.



### Well-Known IDs Table

Lists the currently defined well-known IDs for TCP/UDP port numbers.

### Port Number

Enter the port number for the ID you are defining.

### Protocol

Enter the protocol for the ID you are defining.

### Add Button

Adds the specified ID to the table.

### Clear Button

Clears both the Port Number and Protocol fields, but does not change the content of the table.

### Remove Button

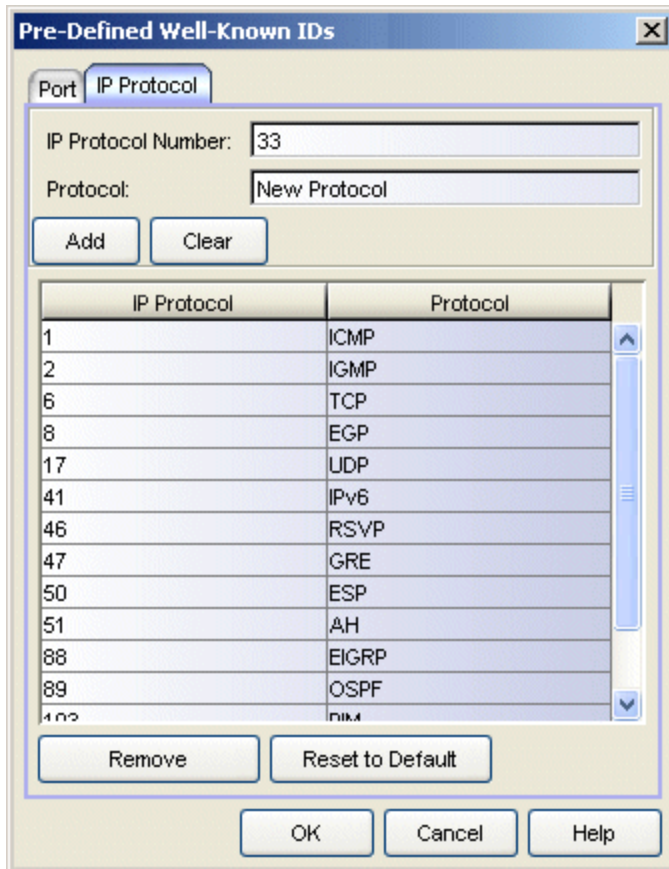
Deletes the selected ID(s) from the list of well-known IDs.

**Reset to Default Button**

Restores the Well-known IDs table to its original settings. Any IDs that you have added will be removed.

**IP Protocol Tab**

The IP Protocol tab lets you define an ID for an IP Protocol type. Once defined, this ID can be used when creating an IP-Protocol rule.

**Well-Known IDs Table**

Lists the currently defined well-known IDs for IP Protocol types.

**IP Protocol Number**

Enter the IP Protocol number for the ID you are defining.

**Protocol**

Enter the protocol for the ID you are defining.

**Add Button**

Adds the specified ID to the table.

**Clear Button**

Clears both the IP Protocol Number and Protocol fields, but does not change the content of the table.

**Remove Button**

Deletes the selected ID(s) from the list of well-known IDs.

**Reset to Default Button**

Restores the Well-known IDs table to its original settings. Any IDs that you have added will be removed.

---

**Related Information**

For information on related tasks:

- [How to Set ACL Manager Options](#)
- [How to Create ACL Rules](#)

## ACL Manager Tab


---

ACL Manager provides the tools that let you efficiently manage the Access Control Lists (ACLs) on your Extreme Networks routers.

ACLs are the containers for the rules that govern network access through your routers. ACL Manager supports five types of ACLs: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. Each ACL type can contain a specific set of rules that define parameters that are appropriate for the devices that they support. Common ACLs can contain rules that are supported by all five types.

To use ACL Manager, you will need to [import](#) the existing ACL data from your devices into ACL Manager. You can import ACL data from a Router Services Database file or from the devices you've modeled in Console. Once you've imported your ACL data, you can use the [ACL Editor](#) to edit and organize your ACLs, and assign ACLs to device interfaces and agent services using the ACL Manager's [interface assignment](#) and [agent assignment](#) views.

It is important to understand that using ACL Manager to manage and assign ACLs does not change the ACLs on the device until the [Enforce](#) operation is used. In ACL Manager you are managing a "view" of your ACLs that is stored in the NetSight database. You will then use the Enforce operation to write that data to the device's active configuration.

At the top left of the ACL Manager tab, there is a menu button  that provides the following options:

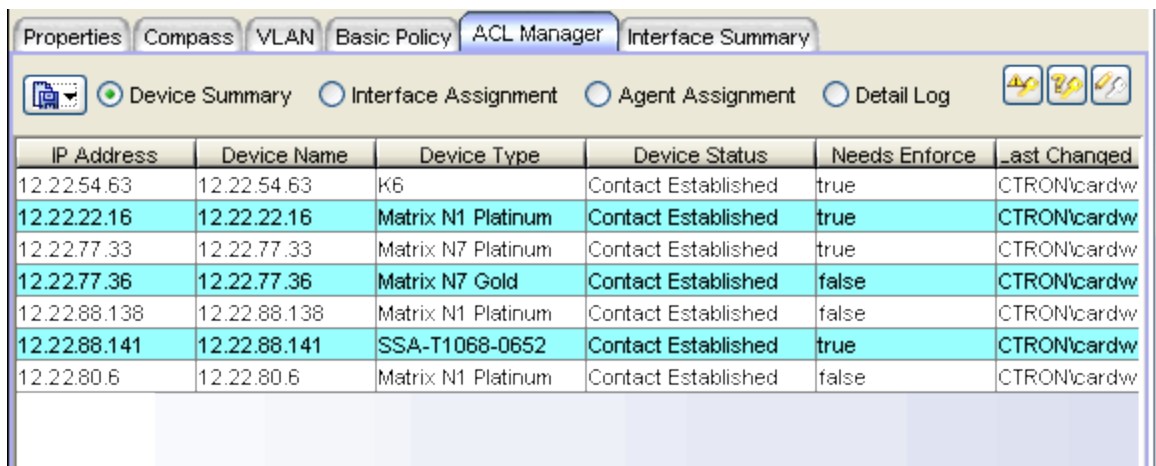
- **Import From RSD** - Opens the RSM Data Importer window where you can select a Router Services Manager Data file to import.
- **Well Knowns** - Opens the Pre-Defined Well-Known IDs window.
- **Options**- Opens the ACL Manager options window where you can view and configure ACL Manager options.
- **Hide Detail Log**- Removes the Detail Log radio button.
- **Show Detail Log** - Adds the Detail Log radio button allowing you to access the Detail Log view.
- **Clear Detail Log** - Clears the Detail Log.

Four views are available in the right panel when the ACL Manager tab is selected. Use the radio buttons at the top of the tab to select the desired view.

- [Device Summary](#)
- [Interface Assignment](#)
- [Agent Assignment](#)
- [Detail Log](#)

## Device Summary

The Device Summary view presents information about the device or devices selected in the left-panel tree that support ACLs.



IP Address	Device Name	Device Type	Device Status	Needs Enforce	Last Changed
12.22.54.63	12.22.54.63	K6	Contact Established	true	CTRON\cardw
12.22.22.16	12.22.22.16	Matrix N1 Platinum	Contact Established	true	CTRON\cardw
12.22.77.33	12.22.77.33	Matrix N7 Platinum	Contact Established	true	CTRON\cardw
12.22.77.36	12.22.77.36	Matrix N7 Gold	Contact Established	false	CTRON\cardw
12.22.88.138	12.22.88.138	Matrix N1 Platinum	Contact Established	false	CTRON\cardw
12.22.88.141	12.22.88.141	SSA-T1068-0652	Contact Established	true	CTRON\cardw
12.22.80.6	12.22.80.6	Matrix N1 Platinum	Contact Established	false	CTRON\cardw

### IP Address

The IP address of the device selected in the left-panel tree.

### Device Name

The name of the device selected in the left-panel tree.

### Device Type

Indicates the type of device.

### Device Status

The contact status for the device.

### Needs Enforce

Indicates whether ACLs need to be enforced on the device: true or false.

The value "Unsupported" is displayed for devices that have been imported into the ACL Manager database (via a Router Services Manager Data file import), but are not supported.



### Last Changed By

Indicates the date and time that the device's ACL data in the database was last changed, and the user that initiated the action. This field is updated when the device data is imported or refreshed and there have been changes to the data, or when a change is made to the ACL data through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

### Last Enforced By

Identifies the user that made the most recent enforce to this device.

### Last Verified By

Identifies the user that performed the most recent verify of the ACLs on this device.



#### ACL Device Enforce Button

Downloads ACLs from the ACL Manager database to the active configuration for enforcement on the currently selected device or devices.



#### ACL Device Verify Button

Lets you compare the ACLs from the selected devices against the current ACLs defined in the ACL Manager database. When the Verify detects a mismatch between ACLs, the Verify Results window opens where you can view differences between the two sets of ACLs.



#### ACL Editor Button

Opens the [ACL Editor window](#) where you can create a new ACL or modify an existing ACL.

## Interface Assignment

The Interface Assignment view presents ACL information for the device interfaces. Use the table editor to change the inbound/outbound ACL value for a selected interface.

IP Address	Display Name	Router	Interface	Primary Address	Secondary Addresses
10.1.210.14	10.1.210.14	Router 1.1.1.1	eth0	10.1.210.14/255.255.....	N/A
10.1.210.14	10.1.210.14	Router 1.1.1.1	vlan.1.1	24.24.24.24/255.255.2...	N/A
10.1.210.14	10.1.210.14	Router 1.1.1.1	vlan.1.2	1.1.1.1/255.255.255.0	N/A
10.1.210.14	10.1.210.14	Router 1.1.1.1	vlan.1.3	3.3.3.3/255.255.255.0	N/A
10.1.210.14	10.1.210.14	Router 1.1.1.1	vlan.1.4	4.4.4.4/255.255.255.0	N/A
10.1.210.14	10.1.210.14	Router 1.1.1.1	vlan.1.5	5.5.5.5/255.255.255.0	N/A
10.20.10.12	xsr1800.fls	Router 1	FastEthernet1	10.20.10.1/255.255.25...	10.20.10.1/255.255.25...
10.20.10.12	xsr1800.fls	Router 1	FastEthernet2	10.20.10.1/255.255.25...	N/A
10.20.10.12	xsr1800.fls	Router 1	Dialer1	1.1.1.1/255.255.255.0	N/A
10.20.10.12	xsr1800.fls	Router 1	Dialer2	2.2.2.2/255.255.255.0	N/A
10.20.10.12	xsr1800.fls	Router 1	Dialer3	3.3.3.3/255.255.255.0	N/A
10.20.10.12	xsr1800.fls	Router 1	Dialer4	4.4.4.4/255.255.255.0	N/A
10.20.10.12	xsr1800.fls	Router 1	Dialer5	5.5.5.5/255.255.255.0	N/A

### IP Address

The IP address of the device selected in the left-panel tree.

### Display Name

The name that is displayed for the device in the left-panel tree.

### Router

The logical router that the interface is assigned to.

### Interface

The interface name.

### Primary Address

Shows the primary IP address for this interface.

### Secondary Addresses

Shows the secondary IP addresses associated with this interface.

### Inbound ACL

Indicates the currently applied inbound ACL for this interface. To change the ACL, click on the Table Editor button to open the Table Editor row at the bottom of the table. Click on the Inbound ACL column in the Table Editor row to open the Select ACL window. Select the desired ACL and click OK. Be sure to [save your changes](#) to the database.

### In Last Changed By

Indicates the date and time that the inbound ACL assignment on this interface was last changed, and the user that initiated the action. This field is updated when the device data is imported or refreshed and there have been changes to the interface assignment, or when a change is made to the interface assignment through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

### Outbound ACL

Indicates the currently applied outbound ACL for the respective interface. To change the ACL, click on the Table Editor button to open the Table Editor row at the bottom of the table. Click on the Outbound ACL column in the Table Editor row to open the Select ACL window. Select the desired ACL and click OK. Be sure to [save your changes](#) to the database.

### Out Last Changed By

Indicates the date and time that the outbound ACL assignment on this interface was last changed, and the user that initiated the action. This field is updated when the device data is imported or refreshed and there have been changes to the interface assignment, or when a change is made to the interface assignment through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

### Description

If supported by the device and interface type, this field contains a description that was entered through the device's local management for this interface.

### Notes

This column provides a place for user-editable notes. Use the [table editor](#) to create the note and then save it to the database.



### Swap In/Outbound ACLs Button

This button swaps the ACLs between the inbound and outbound interfaces, so that the ACL applied to the inbound interface is applied to the outbound interface and vice versa.

**ACL Device Enforce Button**

Downloads ACLs from the ACL Manager database to the active configuration for enforcement on the currently selected device or devices.


**ACL Device Verify Button**

Lets you compare the ACLs from the selected devices against the current ACLs defined in the ACL Manager database. When the Verify detects a mismatch between ACLs, the [ACL Verification Results window](#) opens where you can view differences between the two sets of ACLs.

**ACL Editor Button**

Opens the [ACL Editor window](#) where you can create a new ACL or modify an existing ACL.

**Show/Hide Table Editor Button**

This button toggles the Table Editor row that allows you to change the inbound/outbound ACL value or add a note. When you change a value, a green exclamation mark  marks the cell that has been changed (but not saved to the database) and the Save to Database button becomes active.

**Save to Database Button**

Saves any changes you made in the table to the ACL Manager database.

## Agent Assignment

The Agent Assignment view provides ACL information for the agent services supported on the device: HTTP, SNMP, Telnet, and SSH. Agent services are only supported on Matrix X-Series devices.

IP Address	Display Name	Agent	Agent ACL	Logging	Last Changed By
10.1.106.14	10.1.106.14	http	XSeries	On	CTRON\cardwell on 1206535674663
10.1.106.14	10.1.106.14	snmp	XSeries	On	CTRON\cardwell on 1206535674663
10.1.106.14	10.1.106.14	telnet	XSeries	On	CTRON\cardwell on 1206535674663
10.1.106.14	10.1.106.14	ssh	XSeries	On	CTRON\cardwell on 1206535674663
			XSeries	On	

### IP Address

The IP address of the device selected in the left-panel tree.

### Display Name

The name that is displayed for the device in the left-panel tree.

### Agent

The particular agent (HTML, SNMP, Telnet, SSH) available on the selected device.

### Agent ACL

The name of the ACL that is currently applied to agent traffic on this device. To change the ACL, click on the Table Editor button to open the Table Editor row at the bottom of the table. Click on the Agent ACL column in the Table Editor row to open the Select ACL window. Select the desired ACL and click OK. Be sure to save your changes to the database.

### Logging

This column displays the selected logging capability for the agent traffic on this device. You can use the Table Editor row to change the logging capability. For more information on logging functionality, refer to your router User's Guide.

- **On** - enables logging and displays a message at the device console when traffic is permitted or denied on this interface.
- **Off** - disables logging for traffic on this interface.

- **Deny-only** - enables logging and displays a message at the device console when traffic is denied on this interface.
- **Permit-only** - enables logging and displays a message at the device console when traffic is permitted on this interface.
- **On-syslog** - enables logging and sends a message to the device console and syslog server when traffic is permitted or denied on this interface.
- **Deny-syslog** - enables logging and sends a message to the device console and syslog server when traffic is denied on this interface.
- **Permit-syslog** - enables logging and sends a message to the device console and syslog server when traffic is permitted on this interface.

### Last Changed By

Indicates the date and time that the agent ACL assignment was last changed, and the user that initiated the action. This field is updated when the device data is imported or refreshed and there have been changes to the agent assignment, or when a change is made to the agent assignment through ACL Manager and saved to the database. Keep in mind that the "Last Changed By" field is updated when the database data is updated, not when the device is modified, such as during an enforce.

### Notes

This column provides a place for user-editable notes. Use the [table editor](#) to create the note and then save it to the database.



#### ACL Device Enforce Button

Downloads ACLs from the ACL Manager database to the active configuration for enforcement on the currently selected device or devices.



#### ACL Device Verify Button


Lets you compare the ACLs from the selected devices against the current ACLs defined in the ACL Manager database. When the Verify detects a mismatch between ACLs, the Verify Results window opens where you can view differences between the two sets of ACLs.



#### ACL Editor Button

Opens the [ACL Editor window](#) where you can create a new ACL or modify an existing ACL.

### Show/Hide Table Editor Button

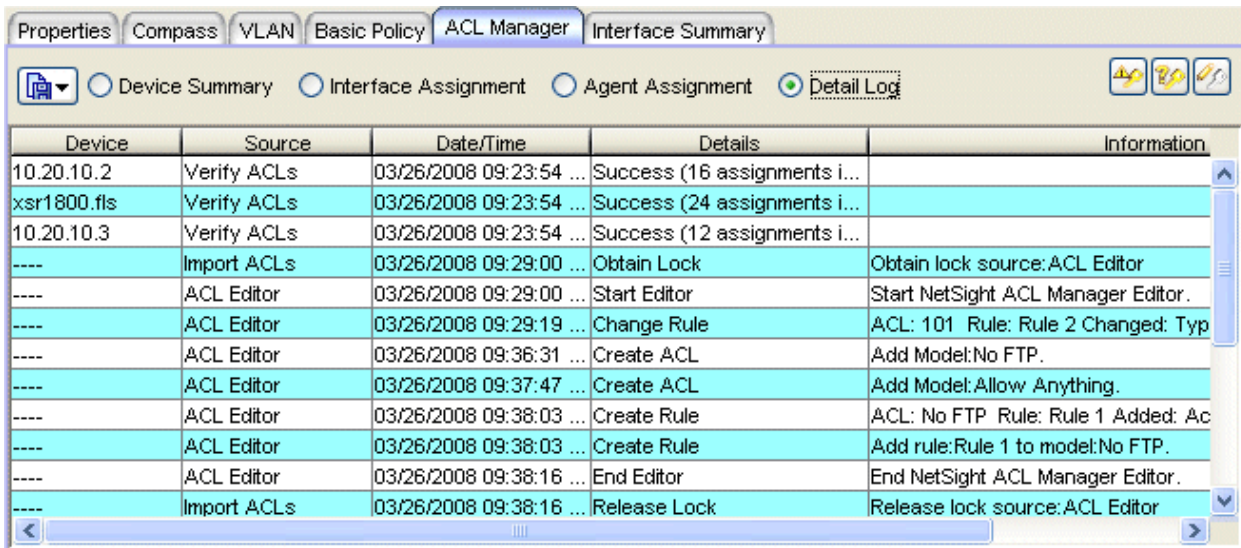
This button toggles the Table Editor row that allows you to change the Agent ACL and Logging values or add a note. When you change a value, a green exclamation mark  marks the cell that has been changed (but not saved to the database) and the Save to Database button becomes active.

### Save to Database Button

Saves any changes you made in the table to the ACL Manager database.

## Detail Log

The Detail Log displays details about ACL Manager actions. You must select Show Detail Log from the drop-down menu in the upper-left corner of the ACL Manager tab in order to see the Detail Log radio button.



Device	Source	Date/Time	Details	Information
10.20.10.2	Verify ACLs	03/26/2008 09:23:54 ...	Success (16 assignments i...	
xsr1800.fl5	Verify ACLs	03/26/2008 09:23:54 ...	Success (24 assignments i...	
10.20.10.3	Verify ACLs	03/26/2008 09:23:54 ...	Success (12 assignments i...	
----	Import ACLs	03/26/2008 09:29:00 ...	Obtain Lock	Obtain lock source:ACL Editor
----	ACL Editor	03/26/2008 09:29:00 ...	Start Editor	Start NetSight ACL Manager Editor.
----	ACL Editor	03/26/2008 09:29:19 ...	Change Rule	ACL: 101 Rule: Rule 2 Changed: Typ
----	ACL Editor	03/26/2008 09:36:31 ...	Create ACL	Add Model:No FTP.
----	ACL Editor	03/26/2008 09:37:47 ...	Create ACL	Add Model:Allow Anything.
----	ACL Editor	03/26/2008 09:38:03 ...	Create Rule	ACL: No FTP Rule: Rule 1 Added: Ac
----	ACL Editor	03/26/2008 09:38:03 ...	Create Rule	Add rule:Rule 1 to model:No FTP.
----	ACL Editor	03/26/2008 09:38:16 ...	End Editor	End NetSight ACL Manager Editor.
----	Import ACLs	03/26/2008 09:38:16 ...	Release Lock	Release lock source:ACL Editor

### Device

The IP address of the device associated with the action.

### Source

The ACL Manager component or process that initiated the action.

### Date/Time

The date and time the action took place.

### Details

Details about the specific action performed.

## Information

Provides additional information about the action.



### ACL Device Enforce Button

Downloads ACLs from the ACL Manager database to the active configuration for enforcement on the currently selected device or devices.



### ACL Device Verify Button

Lets you compare the ACLs from the selected devices against the current ACLs defined in the ACL Manager database. When the Verify detects a mismatch between ACLs, the [ACL Verification Results window](#) opens where you can view differences between the two sets of ACLs.



### ACL Editor Button

Opens the [ACL Editor window](#) where you can create a new ACL or modify an existing ACL.

---

## Related Information

For information on related windows:

- [ACL Editor Window](#)



## ACL Rules Summary

---

ACL Manager supports five types of ACLs: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. Each ACL type can contain a specific set of rules that define parameters that are appropriate for the devices that they support. Common ACLs can contain rules that are supported by all five types.

The specific rules that can be used with each of the ACL types are listed in the following table. The parameters for the rules vary according to Rule Type. For information on configuring the rule parameters click on the rule types listed below.

Rule Type	ACL Type				
	S/K/N 7.x+	N-Series 6.x	X-Series	XSR	Common
<a href="#">AH</a>	Not Available	Available	Not Available	Available	Not Available
<a href="#">ESP</a>	Available	Available	Not Available	Available	Not Available
<a href="#">GRE</a>	Available	Available	Not Available	Available	Not Available
<a href="#">ICMP</a>	Available	Available	Available	Available	Available
<a href="#">IP</a>	Available	Available	Available	Available	Available
<a href="#">IPINIP</a>	Available	Not Available	Available	Not Available	Not Available
<a href="#">IP-Protocol</a>	Available	Available	Not Available	Not Available	Not Available
<a href="#">Standard</a>	Available	Available	Available	Available	Not Available
<a href="#">TCP</a>	Available	Available	Available	Available	Available
<a href="#">UDP</a>	Available	Available	Available	Available	Available

### Related Information

For information on related windows:

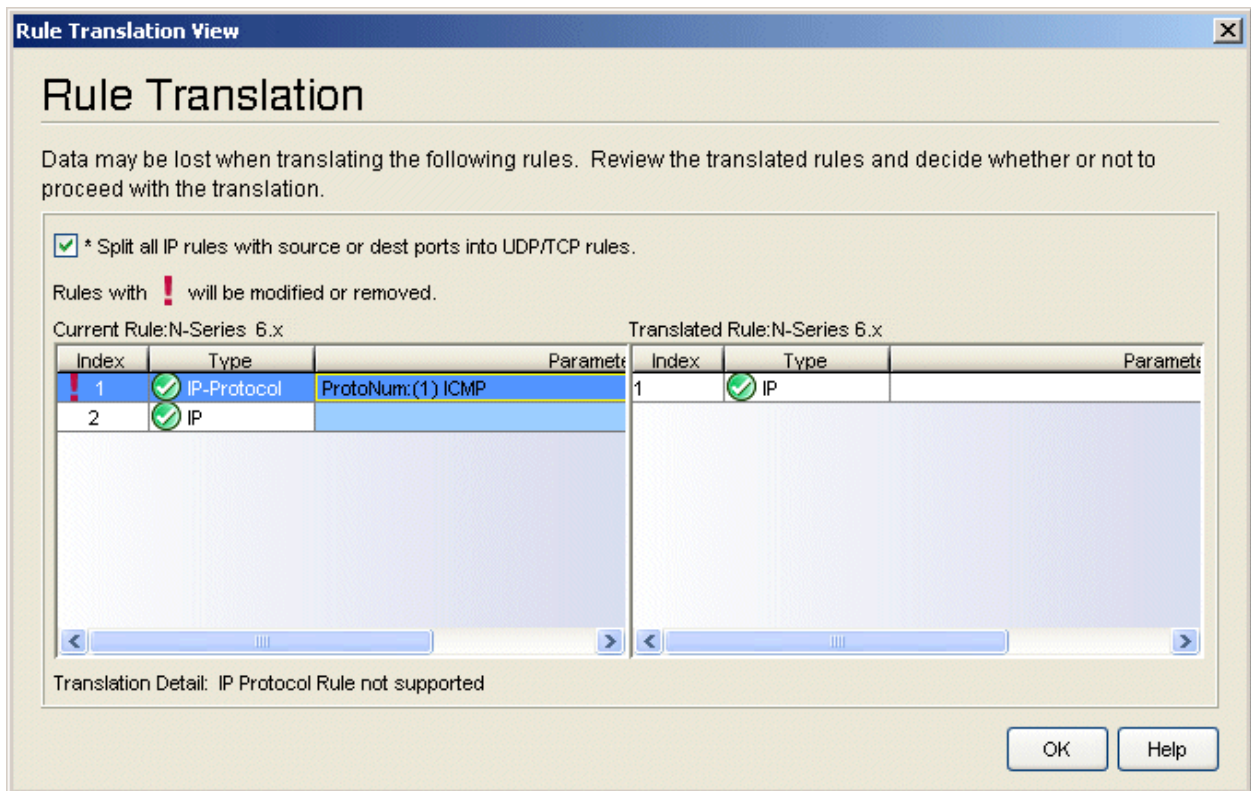
- [Add to ACL/Edit ACL Window](#)

For information on related tasks:

- [How to Create ACL Rules](#)

## ACL Rule Translation View

This view lets you review and make decisions about translation conflicts when pasting incompatible rules that have been cut or copied from one ACL type to another ACL type. Rules that are in conflict appear in the left panel with their original parameters. If the rules being pasted can be translated, they appear in the right panel showing the effects of the translation. Rules that cannot be translated are removed. The translation also offers an option to translate IP rules where a source/destination port is defined, by replacing the single IP rule with a TCP rule and a UDP rule.



### Split all IP rules with source or destination ports into UDP/TCP rules

When checked, IP rules having ports specified will be split into two rules, a UDP rule and a TCP rule that will be the equivalent of the original IP rule.

### Current Rule(s)

This list shows the rules as defined in their original ACL type.

**Index**

Table row reference

**Type**

Rule type in the original ACL type.

**Parameters**

Source, Destination, etc. specified in the original rule.

**Translated Rule(s)**

This list shows the rules after translation.

**Index**

Table row reference

**Type**

Rule type after translation. When IP rules are split, two rules, one UDP and one TCP replace the original IP rule.

**Parameters**

Source, Destination, etc. after translation.

**OK Button**

Performs the translation, pasting both the translated rule(s) and any other compatible rules into the target ACL and closes the Rule Translation View.

---

**Related Information**

For information on related windows:

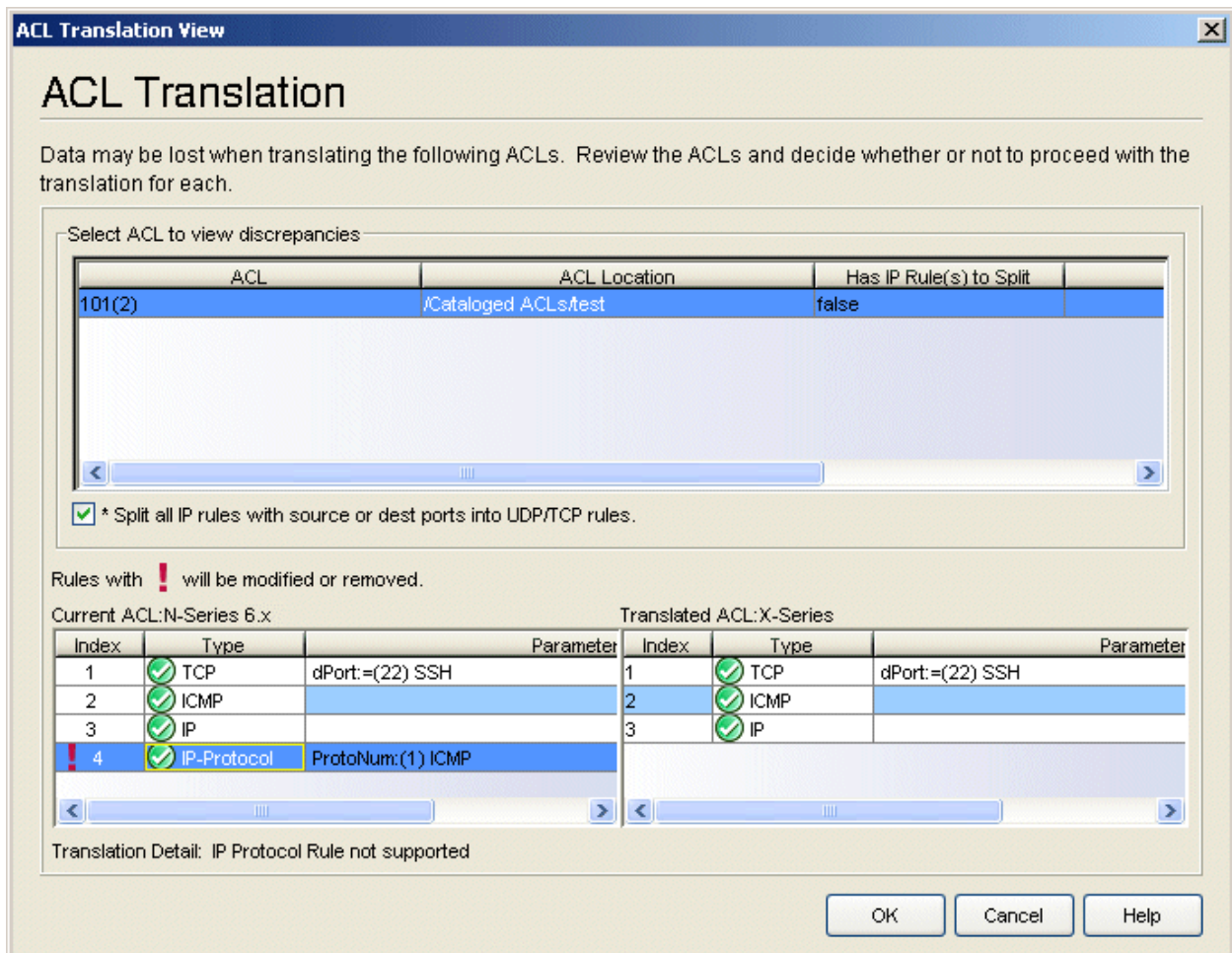
- [ACL Translation View](#)

For information on related tasks:

- [How to Translate ACLs and Rules](#)

## ACL Translation View

This window lets you view translation conflicts when ACLs are being pasted and translated in the [ACL Editor](#) left-panel tree. The top panel lists the ACLs where conflicts exist. The lower-left panel shows the rules for the ACL selected in the top panel with their original parameters. The lower-right panel shows how the rules will be changed if they are translated. The specific rules where a conflict exists appear with a red exclamation mark in the list and a comment below that describes the nature of the conflict. The translation also offers an option to translate IP rules where a source/destination port is defined, by replacing the single IP rule with a TCP rule and a UDP rule.



### Select ACL to view discrepancies

This table lists the ACLs where conflicts exist in the current Paste and Translate operation.

- ACL - This is the ACL Name.
- ACL Location - The path in the ACL Editor tree for this ACL.
- Has IP Rule(s) to Split - Indicates whether the current ACL includes an IP rule where ports are specified: true or false.
- ACLs with the Translate column checked are translated and pasted into the target. ACLs where the Translate checkbox is not checked are not translated, but are also pasted into the target.

### **Split all IP rules with source or destination ports into UDP/TCP rules**

When checked, IP rules having ports specified will be split into two rules, a UDP rule and a TCP rule that will be the equivalent of the original rule.

### **Current ACL**

This table shows the rules in their original ACL type. A red exclamation mark identifies rules that will be modified (split) or removed by translation.

- Index - Table row reference.
- Type - Rule type in the original ACL type.
- Parameters - Source, Destination, etc. specified in the original ACL type.

### **Translated ACL**

This table shows the rules as they will be in the translated ACL.

- Index - Table row reference.
  - Type - Rule type in the translated ACL type.
  - Parameters - Source, Destination, etc. in the translated ACL type.
- 

## **Related Information**

For information on related windows:

- [How to Manage ACLs](#)
- [Rule Translation View](#)

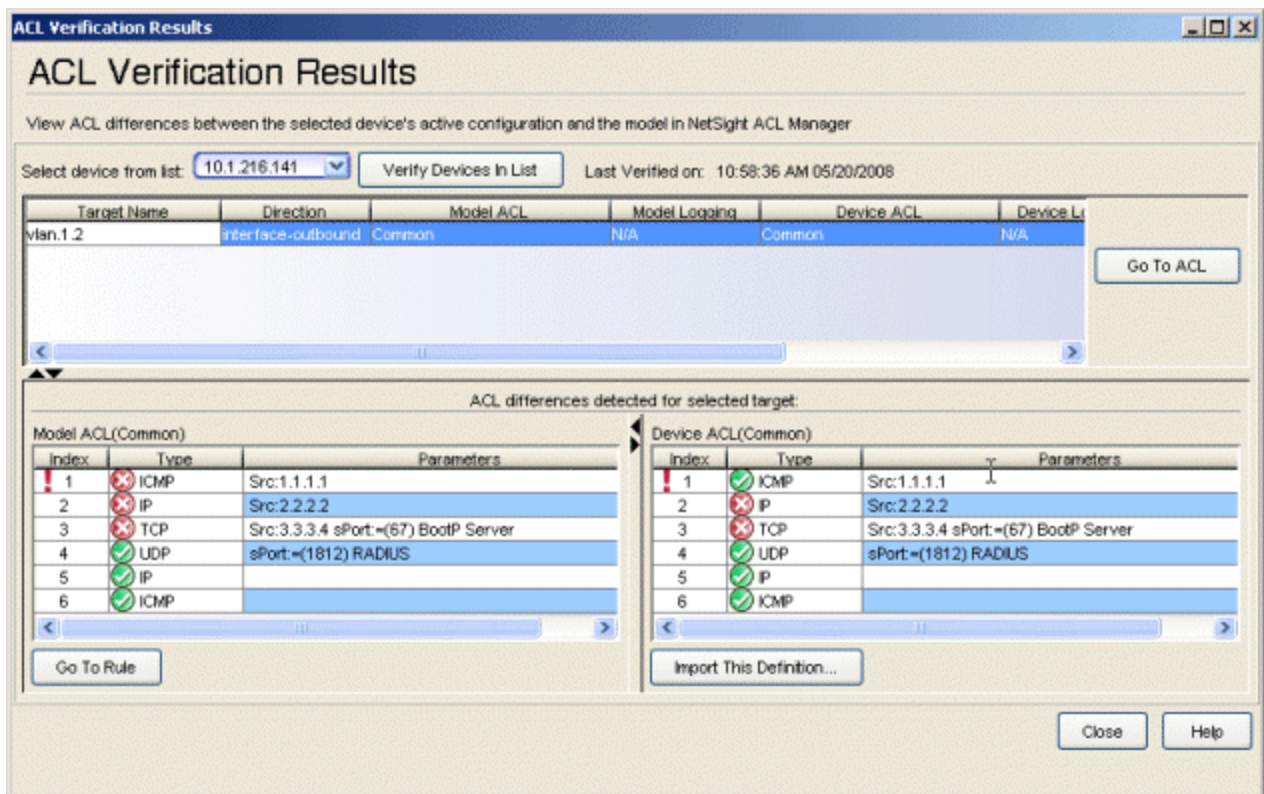
For information on related tasks:

- [How to Translate ACLs and Rules](#)

## ACL Verification Results Window

The Verify operation lets you compare the ACLs from selected devices against the current ACLs defined in the ACL Manager database. When the Verify operation detects a mismatch between ACLs, the ACL Verification Results window opens where you can view the differences between the selected device's active configuration and the model in ACL Manager.

The window consists of three panels. The top panel lists the interfaces where there are differences between the ACLs. When an interface is selected from the top list, the lower-right panel shows the ACLs applied to the interface in the device (Device ACL) and the lower-left panel shows the ACLs for the interface that are stored in the ACL Manager database (Model ACL). Differences between the Device ACL and Model ACL are highlighted by a red exclamation mark (!).



### Select device from list:

This drop-down list contains all of the devices where ACL Manager detected a difference between the ACLs in a device's active configuration

and the ACLs applied to that device in ACL Manager's database. The drop-down list lets you select from the list of devices and show the particular targets in the Target table.

**Last Verified on**

Shows the time and date of the last Verify operation.

**Target Table**

This table lists the targets where there are differences between the ACL definitions in ACL Manager and the ACLs applied in the selected device.

**Model ACL Table**

This table lists the rules defined in the ACL Manager database for the currently selected ACL and uses a red exclamation mark (!) to indicate those that are different from the rules in the ACL applied on the device .

**Device ACL Table**

This table lists the rules defined in the device for the currently selected ACL and uses a red exclamation mark (!) to indicate those that are different from the rules defined in ACL Manager's database.

**Verify Devices in List**

During the verification process, if you edit or delete rules in an ACL, use this button to update the ACL Verification Results Window. It reads the ACLs currently in effect (enforced) on all the devices on the device list and compares them against the ACLs you have defined in the ACL Manager database. Interfaces where there are differences are listed in the Target table. Interfaces where the differences have been resolved are removed from the list. When no differences exist, the ACL Verification Results window is closed.

**Go to ACL**

Clicking this button opens the [ACL Editor](#) with the target ACL selected.

**Go to Rule**

Clicking this button opens the [ACL Editor](#) with the database rule selected.

**Import This Definition**

Copies the rules from the Device ACL table into the Model ACL table. Clicking this button opens the [Import This Definition window](#) where you can specify certain options for the import. After importing the ACL definition from the device, the Model ACL and Device ACL tables are the same and verifying ACLs again will result in the interface from which the ACL definitions were imported, no longer appearing in the interface table at the top of the window.

### **Related Information**

For information on related tasks:

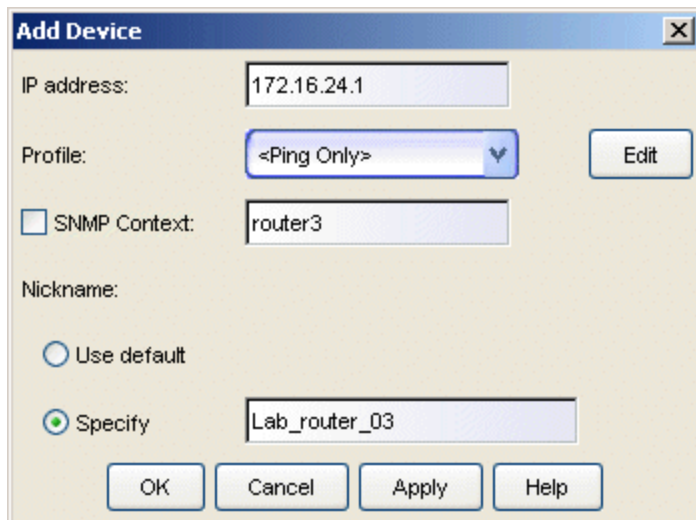
- [How to Verify ACLs](#)



## Add Device Window

---

The Add Device window lets you add a device to the NetSight database and place it in a selected group in the left panel. You can access this window by right-clicking a group in the left panel and choosing **Add Device** from the **Edit** menu or from the right-click menu.



### IP Address

The IP address of the device being added.

### Profile

This drop-down list lets you select one of the SNMP profiles that have been defined for device access. The Edit button lets you create a profile if one does not already exist.

### SNMP Context

When checked, you can specify a SNMP context that has been configured on a device. An SNMP context is a collection of MIB objects, often associated with a network entity. The SNMP context lets you access a subset of MIB objects related to that context. Console lets you specify a SNMP Context for both SNMPv1/v2 and SNMPv3.

The use of context differs depending on the protocol version being used with a user's credentials:

- When used, with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.
- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, an SNMPv1 or SNMPv2 community name can be mapped, through Local Management, to a particular SNMP context on the device. Thus, when SNMPv1/v2 credentials are used with a Context entry, access is granted to the subset of MIB objects associated with that credential (community name). If the credential used is accepted, but the context specified doesn't match a context configured on the device, access is granted to the default context.

Console treats each context for a given device (IP address) as a distinct device. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to your device configuration guide for more information about setting and showing SNMP contexts.

### Nickname

You can use the default nickname or click **Specify** to assign a unique nickname to this device. The default nickname for SNMP devices is the *sysName* MIB object, or if no *sysName* has been assigned, the device's IP address. The default nickname for pingable devices is the IP address.

### Edit Button

Opens the Authorization Configuration window where you can add or modify an existing profile to be associated with this device.

---

## Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)

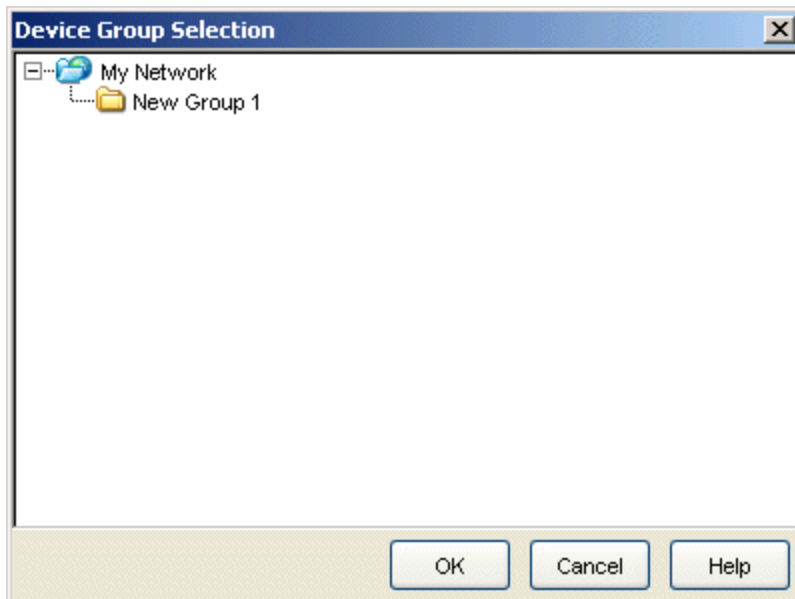
For information on related tasks:

- [How to Add, Remove, and Delete Devices](#)
- [How to Add, Remove, and Rename Groups](#)

## Add Device(s) to a Group Window

---

The Add Device(s) to a Group window lets you add devices selected from a [FlexView](#) table to a user-created group in the left panel. Use this panel to select the group to which you want to add the selected devices. See [How to Add, Remove, and Delete Devices](#) for more information.



---

### Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)
- [FlexView Tab](#)

For information on related tasks:

- [How to Add, Remove, and Delete Devices](#)
- [How to Add, Remove, and Rename Groups](#)

## Add to ACL / Edit ACL Window

---

Use this window to either add a new rule to the selected ACL or edit an existing rule in an ACL. You can access this window from the [ACL Editor](#) by clicking the **New** or **Edit** button in the right-panel Editor tab.

ACL Manager supports five types of ACLs: S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common. Each ACL type can contain a specific set of rules that define parameters that are appropriate for the devices that they support. Common ACLs can contain rules that are supported by all five types. The rule types that can be used with each of the five ACL types are listed in the [ACL Rules Summary](#).

The parameters/fields in this window will change according to the rule type selected. This help topic provides information for each of the following rule types:

- [AH, ESP, or GRE](#)
- [ICMP or IP](#)
- [IPINIP](#)
- [IP-Protocol](#)
- [Standard](#)
- [TCP or UDP](#)

### AH, ESP, or GRE Rules

AH, ESP, and GRE rules can be applied to allow or block AH, ESP, and GRE traffic from entering or leaving a router port. The rule definitions for AH, ESP, and GRE traffic share the same parameters. ESP and GRE rules can only be created in S/K/N 7.x+, N-Series 6.x, and XSR ACLs. AH rules can only be created in N-Series 6.x and XSR ACLs.

Sample ESP rule.
**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

**Action**

**Permit** - allow AH, ESP, or GRE traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block AH, ESP, or GRE traffic that matches the parameters in this rule from entering or leaving the port where this rule is applied.

**Remark** - allows you to add a remark to the ACL. (Available on S-Series, K-

Series, and N-Series devices with 7.x firmware only.)

If the Comment checkbox is checked, the rule will be commented out (disabled).

### ACL Type

Identifies the type of ACL the rule is being created for.

### Source Address

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Destination Address

Allow or block packets with this destination address, based on the selected Action (permit/deny). This parameter can be defined as **Any** destination address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Mask

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source or destination address in the header of the packet are ANDed with the associated mask and compared against the source/destination address fields. For example, if you entered 172.90.00.00 into the Source/Destination field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

### TOS

Allow or block packets with these ToS (Type of Service) or DSCP (Diffserv Codepoint) values, based on the selected Action (permit/deny). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame.

- TOS - allow or block packets with the TOS value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 255.

- Precedence - allow or block packets with the Precedence value specified here. You can select one of the pre-defined values or specify a precedence value of 0-7.
- DSCP - allow or block packets with the DSCP value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 63.

---

**NOTE:** IPv4 defines the ToS field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

---

### Enable Logging/Enable Verbose Logging

These checkboxes let you enable or disable logging or detailed (verbose) logging for this rule. (Verbose logging is available on S-Series, K-Series, and N-Series devices with 7.x firmware only.) When enabled, a Log message is sent to the device console and if you have a Syslog server configured, the same message is sent to the Syslog server. For more information on logging functionality, refer to your router User's Guide.

### Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

## ICMP or IP Rules

ICMP and IP rules share most of the same parameters, however different parameters apply to the rules depending on which type of ACL they are created for. These rules allow or block ICMP or IP traffic from entering or leaving a router port.

Sample ICMP rule.

**Add to ACL:N-Series**

Name:

Action:   Comment:

ACL Type: N-Series 6.x

Rule Type:

Source Address:  /  CIDR

Destination Address:  /  CIDR

TOS

TOS  Pre-Defined:   Specify Number:

Precedence  Pre-Defined:   Specify Number:

DSCP  Pre-Defined:   Specify Number:

Message

Type:

Code:

Enable Logging

Notes:

**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

**Action**

**Permit** - allow ICMP/IP traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block ICMP/IP traffic that matches the parameters in this rule from entering or leaving the port where this rule is applied.

**Remark** - allows you to add a remark to the ACL. (Available on S-Series, K-



Series, and N-Series devices with 7.x firmware only.)

If the Comment checkbox is checked, the rule will be commented out (disabled).

### ACL Type

Identifies the type of ACL the rule is being created for.

### Source Address

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Destination Address

Allow or block packets with this destination address, based on the selected Action (permit/deny). This parameter can be defined as **Any** destination address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Mask

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source or destination address in the header of the packet are ANDed with the associated mask and compared against the source/destination address fields. For example, if you entered 172.90.00.00 into the Source/Destination field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

### TOS

Allow or block packets with these ToS (Type of Service) or DSCP (Diffserv Codepoint) values, based on the selected Action (permit/deny). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame.

- TOS - allow or block packets with the TOS value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 255.

- Precedence - allow or block packets with the Precedence value specified here. You can select one of the pre-defined values or specify a precedence value of 0-7.
- DSCP - allow or block packets with the DSCP value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 63.

---

**NOTE:** IPv4 defines the ToS field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

---

### Message

ICMP rules can be defined to allow or reject traffic based on ICMP Message Type (0 to 255). When a Message Type is specified, an optional ICMP Message Code (1 to 255) can be used to create a more specific rule.

### Enable Logging

These checkboxes let you enable or disable logging or detailed (verbose) logging for this rule. (Verbose logging is available on S-Series, K-Series, and N-Series devices with 7.x firmware only.) When enabled, a Log message is sent to the device console and if you have a Syslog server configured, the same message is sent to the Syslog server. For more information on logging functionality, refer to your router User's Guide.

### Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

## IPINIP Rules

IPINIP rules allow or block IPINIP traffic from entering or leaving a router port. This type of rule can only be created in S/K/N 7.x+ and X-Series ACLs.

Sample IPINIP rule.

**Add to ACL:X-Series**

Name:

Action:   Comment:

ACL Type: X-Series

Rule Type:

Source Address:  /  /  CIDR

Destination Address:  /  /  CIDR

TOS

TOS  Pre-Defined:   Specify Number:

Precedence  Pre-Defined:   Specify Number:

DSCP  Pre-Defined:   Specify Number:

Enable Logging

Notes:

**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

**Action**

**Permit** - allow IPINIP traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block IPINIP traffic that matches the parameters in this rule from

entering or leaving the port where this rule is applied.

If the Comment checkbox is checked, the rule will be commented out (disabled).

### ACL Type

Identifies the type of ACL the rule is being created for.

### Source Address

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Destination Address

Allow or block packets with this destination address, based on the selected Action (permit/deny). This parameter can be defined as **Any** destination address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Mask

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source or destination address in the header of the packet are ANDed with the associated mask and compared against the source/destination address fields. For example, if you entered 172.90.00.00 into the Source/Destination field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

### TOS

Allow or block packets with these ToS (Type of Service) or DSCP (Diffserv Codepoint) values, based on the selected Action (permit/deny). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame.

- TOS - allow or block packets with the TOS value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 255.

- Precedence - allow or block packets with the Precedence value specified here. You can select one of the pre-defined values or specify a precedence value of 0-7.
- DSCP - allow or block packets with the DSCP value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 63.

---

**NOTE:** IPv4 defines the ToS field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

---

### Enable Logging

This check box lets you enable or disable logging for this rule. When enabled, a Log message is sent to the console and if you have a Syslog server configured, the same message is sent to the Syslog server.

### Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

## IP-Protocol Rules

IP-Protocol rules allow or block specific IP traffic from entering or leaving a router port. They can be used to define rules that specify any valid IP protocol other than those specified in other rules, (IP, ICMP, TCP, and UDP). For example, to specify a rule for IP encapsulation in IP, you can use IP protocol type 4 in the rule. IP-Protocol rules are only supported for S/K/N 7.x+ and N-Series 6.x ACLs.

Sample IP-Protocol rule.

**Add to ACL:N-Series**

Name:

Action:   Comment:

ACL Type: N-Series 6.x

Rule Type:

Source Address:   /   CIDR

Destination Address:   /   CIDR

IP Protocol Number

Pre-Defined:   Specify Number:

TOS

TOS  Pre-Defined:   Specify Number:

Precedence  Pre-Defined:   Specify Number:

DSCP  Pre-Defined:   Specify Number:

Enable Logging

Notes:

**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

**Action**

**Permit** - allow IP-Protocol traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block IP-Protocol traffic that matches the parameters in this rule from entering or leaving the port where this rule is applied.

**Remark** - allows you to add a remark to the ACL. (Available on S-Series, K-Series, and N-Series devices with 7.x firmware only.)

If the Comment checkbox is checked, the rule will be commented out (disabled).

**ACL Type**

Identifies the type of ACL the rule is being created for.

**Source Address**

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

**Destination Address**

Allow or block packets with this destination address, based on the selected Action (permit/deny). This parameter can be defined as **Any** destination address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

**Mask**

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source or destination address in the header of the packet are ANDed with the associated mask and compared against the source/destination address fields. For example, if you entered 172.90.00.00 into the Source/Destination field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

**IP Protocol Number**

Select a Pre-Defined protocol or enter a number (1-255).

## TOS

Allow or block packets with these ToS (Type of Service) or DSCP (Diffserv Codepoint) values, based on the selected Action (permit/deny). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame.

- TOS - allow or block packets with the TOS value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 255.
- Precedence - allow or block packets with the Precedence value specified here. You can select one of the pre-defined values or specify a precedence value of 0-7.
- DSCP - allow or block packets with the DSCP value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 63.

---

**NOTE:** IPv4 defines the ToS field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

---

## Enable Logging

These checkboxes let you enable or disable logging or detailed (verbose) logging for this rule. (Verbose logging is available on S-Series, K-Series, and N-Series devices with 7.x firmware only.) When enabled, a Log message is sent to the device console and if you have a Syslog server configured, the same message is sent to the Syslog server. For more information on logging functionality, refer to your router User's Guide.

## Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

## Standard Rules

Standard rules can be applied to allow or block IP traffic from a specific source address from entering or leaving a router port. A Standard rule cannot be created in Common ACLs.



*Sample Standard rule.*

**Add to ACL:X-Series**

Name:

Action:   Comment:

ACL Type: X-Series

Rule Type:

Source Address

/  CIDR

Enable Logging

Notes:

**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

**Action**

**Permit** - allow IP traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block IP traffic that matches the parameters in this rule from entering or leaving the port where this rule is applied.

If the Comment checkbox is checked, the rule will be commented out (disabled).

**ACL Type**

Identifies the type of ACL the rule is being created for.

### Source Address

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Mask

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source address in the header of the packet are ANDed with the associated mask and compared against the source address field. For example, if you entered 172.90.00.00 into the Source field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

### Enable Logging

This check box lets you enable or disable logging for this rule. When enabled, a Log message is sent to the console and if you have a Syslog server configured, the same message is sent to the Syslog server.

### Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

## TCP or UDP Rules

TCP and UDP rules allow or block TCP or UDP traffic from entering or leaving a router port. TCP and UDP rules can be created in S/K/N 7.x+, N-Series 6.x, X-Series, XSR, and Common ACLs. When created for S/K/N 7.x+, N-Series 6.x, and X-Series ACLs, these rules provide additional settings for Type of Service and Logging.

*Sample TCP rule.*

**Add to ACL:N-Series**

Name:

Action:   Comment:

ACL Type: N-Series 6.x

Rule Type:

Source Address:  /  CIDR

Destination Address:  /  CIDR

TCP/UDP Port(s)

Source:   -

Destination:   -

TOS

TOS  Pre-Defined:   Specify Number:

Precedence  Pre-Defined:   Specify Number:

DSCP  Pre-Defined:   Specify Number:

Established

Enable Logging

Notes:

**Name**

The name given to this rule. The name is a string of up to 100 characters or numbers and is usually descriptive of the rule's function. This name is not used in the device. Rather, it serves as a means of identifying rules in ACL Manager.

### Action

**Permit** - allow TCP/UDP traffic that matches the parameters in this rule to enter or leave the port where this rule is applied.

**Deny** - block TCP/UDP traffic that matches the parameters in this rule from entering or leaving the port where this rule is applied.

**Remark** - allows you to add a remark to the ACL. (Available on S-Series, K-Series, and N-Series devices with 7.x firmware only.)

If the Comment checkbox is checked, the rule will be commented out (disabled).

### ACL Type

Identifies the type of ACL the rule is being created for.

### Source Address

Allow or block packets with this source address, based on the selected Action (permit/deny). This parameter can be defined as **Any** source address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Destination Address

Allow or block packets with this destination address, based on the selected Action (permit/deny). This parameter can be defined as **Any** destination address, a specific IP address or, as a subnet or range of addresses when used with the associated Mask parameter. Typing a **slash** after entering an address advances the entry marker to the mask field and automatically enters a mask (based on the address).

### Mask

The mask is used as a filter to define a range of IP addresses. Masks can be entered as CIDR or dotted-decimal format. Address bits from a source or destination address in the header of the packet are ANDed with the associated mask and compared against the source/destination address fields. For example, if you entered 172.90.00.00 into the Source/Destination field and typed 255.255.0.0 as the associated mask, then all incoming packets in the range 172.90.00.00 through 172.90.255.255 would result in an address match.

### Source Port

Filter or forward packets using this source port argument, based on the selected Action (permit/deny). You can set the source port as **Any** source TCP/UDP port, select a TCP/UDP type from the list of well-known values,

or select **Other** and manually enter the value in decimal form. TCP/UDP port address. You can also enter a range of values. (TCP/UDP port numbers are defined in RFC 1700.)

---

**TIP:** You can define a new value for a TCP/UDP port number using the Pre-Defined Well-Known IDs window. Once defined, it is available for selection from the list of well-known values.

---

### Destination Port

Filter or forward packets using this destination port argument, based on the selected Action (permit/deny). You can set the destination port as **Any** source TCP/UDP port, select a TCP/UDP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. TCP/UDP port address. You can also enter a range of values. (TCP/UDP port numbers are defined in RFC 1700.)

### TOS

Allow or block packets with these ToS (Type of Service) or DSCP (Diffserv Codepoint) values, based on the selected Action (permit/deny). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service for each frame.

- TOS - allow or block packets with the TOS value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 255.
- Precedence - allow or block packets with the Precedence value specified here. You can select one of the pre-defined values or specify a precedence value of 0-7.
- DSCP - allow or block packets with the DSCP value specified here. You can select from the pre-defined values or specify a decimal number between 0 and 63.

---

**NOTE:** IPv4 defines the ToS field as setting the Precedence and Type of Service requested for a packet. IPv6 redefined this field as the DS (Differentiated Service) field containing a DSCP (Differentiated Service Codepoint) value, to define Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

---

### Established

Indicates whether this rule will allow TCP/UDP responses through the router, provided the connection between two hosts is already established.

### Enable Logging

These checkboxes let you enable or disable logging or detailed (verbose) logging for this rule. (Verbose logging is available on S-Series, K-Series, and N-Series devices with 7.x firmware only.) When enabled, a Log message is sent to the device console and if you have a Syslog server configured, the same message is sent to the Syslog server. For more information on logging functionality, refer to your router User's Guide.

### Notes

Enter a description of the rule. This information will be displayed in the Editor tab in the [ACL Editor](#).

Swap 

Exchanges the Source and Destination Address parameters. The source address and mask become the destination address and mask and vice-versa.

Swap Source/Dest Ports 

Exchanges the Source and Destination Port parameters. The source port parameters become the destination port parameters and vice-versa.

---

### Related Information

For information on related windows:

- [ACL Editor](#)
- [ACL Rules Summary](#)

For information on related tasks:

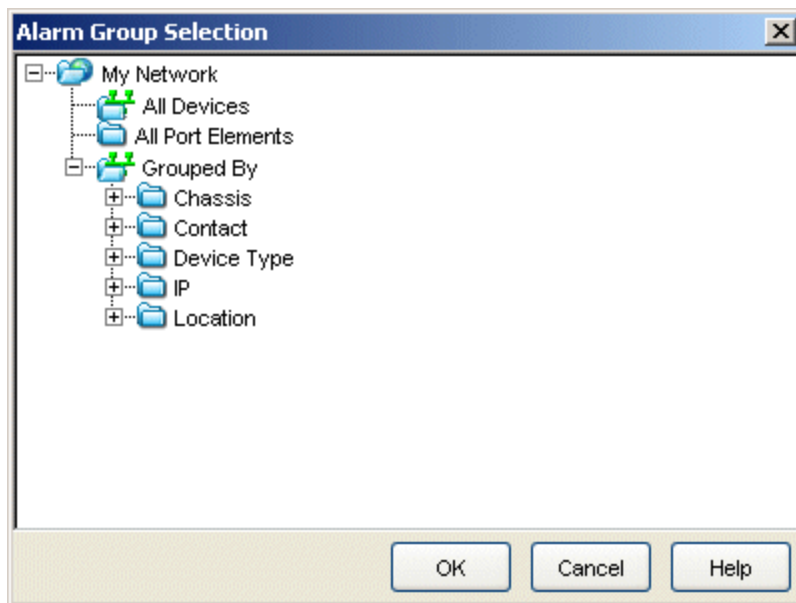
- [How to Create ACL Rules](#)

## Alarm Group Selection Window

---

This window lets you select one or more device groups in the Console device tree. The device group can include [port elements](#), if desired. Only the devices or port elements in those groups will be monitored for the criteria you have configured for the alarm. You can multi-select device groups using the Ctrl key.

The window is accessed from the **Select Groups** button in the [Alarms Manager window](#).



---

### Related Information

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)

## Alarm History Window (Legacy)

---

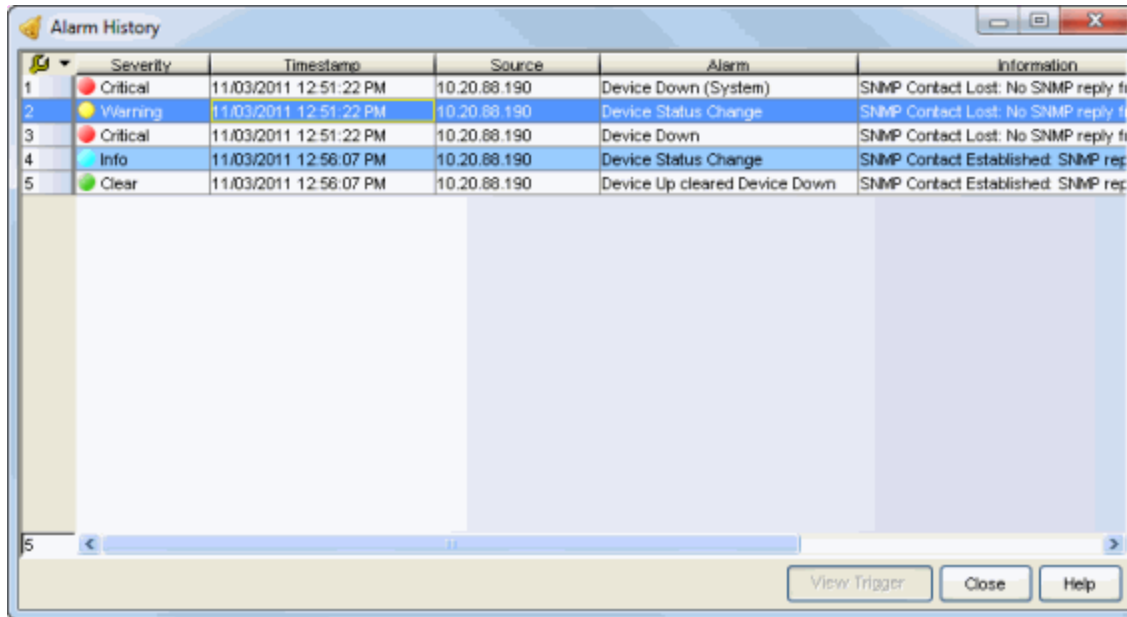
Extreme Management Center records alarm information whenever an alarm is raised and whenever an alarm is cleared, and displays the records in the Alarm History window, allowing you to view information about current and past alarms.

If a triggering event is stored with a selected history record, you can view the event by clicking the View Trigger button. If there is no triggering event, the button is disabled. You can enable an option to preserve alarm triggering events and store them with the alarm history record in the Suite-Wide Alarm Configuration options (Tools > Options > Suite > Alarm Configuration).

You can access the Alarm History from Console and Management Center.

- In the Console **Event View Alarms** tab, use the **All Alarm History** button to view information about all current and past alarms, or right-click on an alarm to view an alarm history for that specific alarm.
- In the Management Center **Alarms** tab, click on a Source link to view an alarm history for that device or click on the Alarm Name link to view a history for that specific alarm.
- In the Management Center **Network** tab, right-click on a device and select Alarm History from the menu to view an alarm history for that device.
- In the Management Center Interface Summary view, right-click on an interface and select Alarm History from the menu to view an alarm history for that interface.





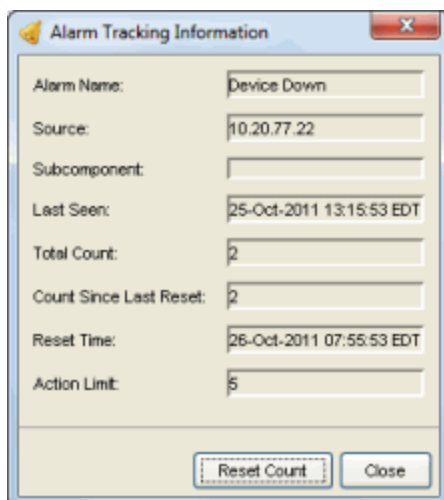
	Severity	Timestamp	Source	Alarm	Information
1	Critical	11/03/2011 12:51:22 PM	10.20.88.190	Device Down (System)	SNMP Contact Lost: No SNMP reply fi
2	Warning	11/03/2011 12:51:22 PM	10.20.88.190	Device Status Change	SNMP Contact Lost: No SNMP reply fi
3	Critical	11/03/2011 12:51:22 PM	10.20.88.190	Device Down	SNMP Contact Lost: No SNMP reply fi
4	Info	11/03/2011 12:58:07 PM	10.20.88.190	Device Status Change	SNMP Contact Established: SNMP rep
5	Clear	11/03/2011 12:58:07 PM	10.20.88.190	Device Up cleared Device Down	SNMP Contact Established: SNMP rep

5

View Trigger Close Help

## Alarm Limits

If alarm [action limits](#) have been enabled for an alarm (in the [Actions subtab](#) of the Alarms Manager window), you can right-click on an alarm history record and select Alarm Limits to open the Alarm Tracking Information window (shown below). This window displays the configured action limit, the number of times the action has been taken (Total Count), the number of times the action has been taken since the last reset, and the time of the next reset. You can also manually reset the alarm limit count using the **Reset Count** button. This resets the count for only this alarm on only this device or interface.



Alarm Name:	Device Down
Source:	10.20.77.22
Subcomponent:	
Last Seen:	25-Oct-2011 13:15:53 EDT
Total Count:	2
Count Since Last Reset:	2
Reset Time:	26-Oct-2011 07:55:53 EDT
Action Limit:	5

Reset Count Close

## Alarm History Options

You can change certain alarm history parameters in the Suite-Wide Alarm Configuration options (Tools > Options > Suite > Alarm Configuration).

- By default, the alarm history is maintained for 14 days. You can change the number of days in the options.
  - By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared. In the options, you can enable a Detailed Alarm History, so that repeat occurrences of an alarm being raised will also be recorded.
  - You can enable an option to preserve alarm triggering events, so that any triggering events are stored with the alarm history record. If a triggering event is stored with the currently selected history record, you can view the event by clicking the View Trigger button in the Alarm History window. If there is no triggering event, the button is disabled.
- 

### Related Information

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)

## Alarms Manager Window

---

The Alarms Manager window allows you to configure the network alarms that provide status information for a particular problem or condition on a particular network component. Alarms are triggered when certain trap or event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed.

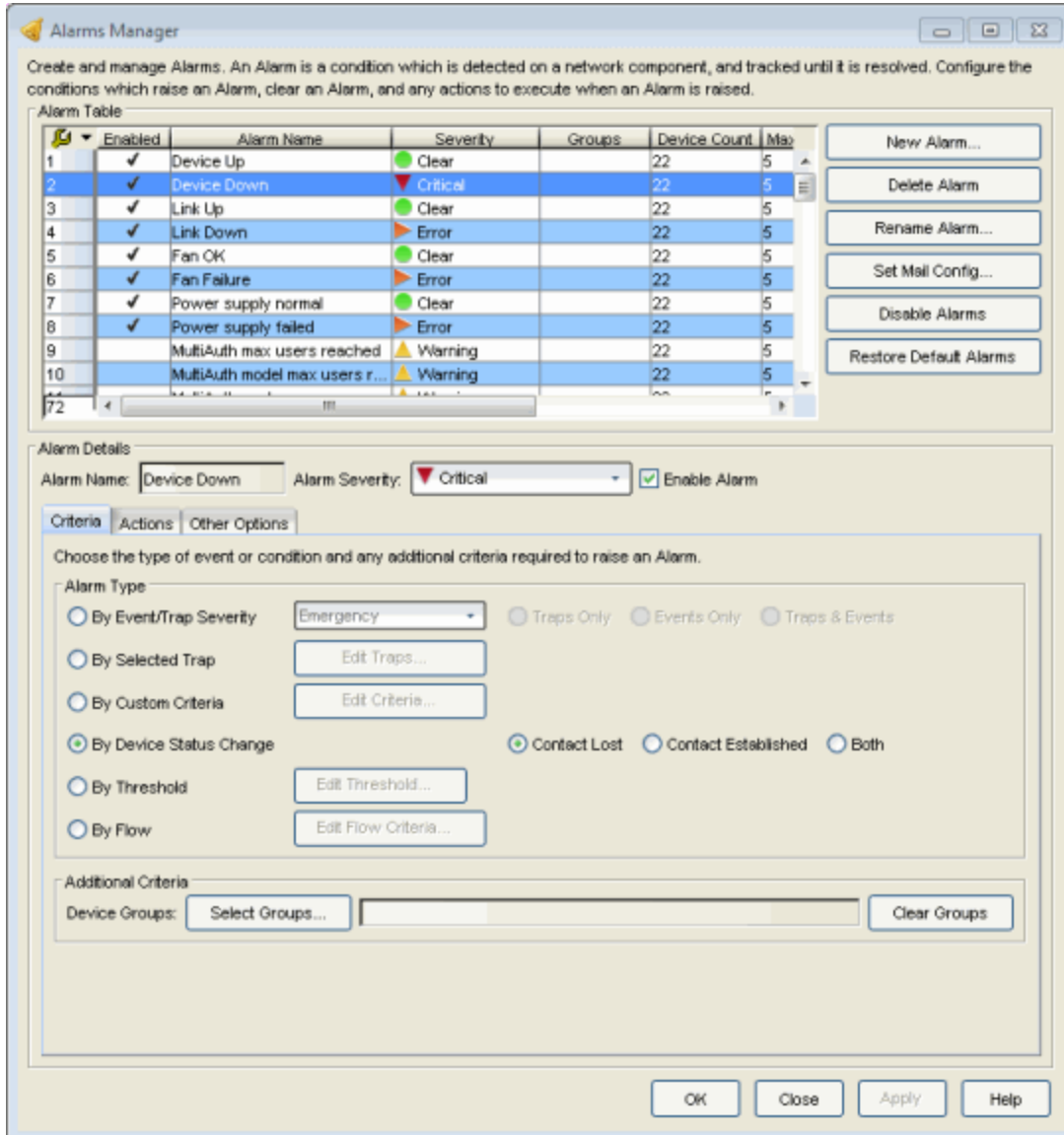
Use this window to add a new alarm definition, which includes configuring the conditions (criteria) which will trigger the alarm, and defining the actions that will be automatically performed to notify a person or network component about the problem, when the alarm is triggered.

You can create an alarm definition that detects a problem or condition and raises an alarm, and you can also create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Link Down alarm is triggered when a device emits a linkDown trap. Then, when the device emits a linkUp trap, the Link Up alarm automatically clears the Link Down alarm.

Extreme Management Center ships with a set of default alarm definitions, which you can see listed in the Alarm Table at the top of the window. You can use these default alarms as is, or delete or modify them as desired.

For complete instructions on configuring alarms, see [How to Configure Alarms](#).

You can access this window from the Tools > Alarm/Event > Alarms Manager menu option.









## Alarm Details

### Alarm Name

The name of the alarm.

### Alarm Severity

Use this drop-down list to select a severity level for the alarm. The alarm can have its own specified severity regardless of the severity of the event or trap that triggered it.

-  (question mark) Set from Source - the alarm will use the severity level of the trigger event, for example a warning event.
-  (Red) Critical - A problem with significant implications.
-  (Orange) Error - A problem with limited implications.
-  (Yellow) Warning - A condition that might lead to a problem.
-  (Blue) Info - Information only; not a problem.
-  (Green) Clear - An alarm that clears another alarm (for example, LinkUp).

### Enable Alarm

Select the Enable Alarm checkbox to activate the alarm. You can disable an alarm to deactivate it without deleting the definition. You can see whether an alarm is enabled looking at the Enabled checkbox in the table.

### *Criteria Subtab*

Use this tab to specify the alarm event that will trigger the alarm.

### By Event/Trap Severity

This option lets you select the trap/event severity that will trigger the alarm: **Emergency, Alert, Critical, Error, Warning, Notice, or Info**. You can also select whether the alarm will be triggered by traps or events, or both.

### By Selected Trap

This option lets you open the [Trap Selection window](#) where you can select one or more trap that will trigger the alarm. You will be able to select from all the Trap IDs available for the devices modeled in the Management Center database.

### By Custom Criteria

This option lets you open the [Edit Custom Alarm Criteria window](#) where you can define very specific criteria to trigger the alarm.

### By Device Status Change

This option lets you specify a device status change to trigger the alarm. **Contact Lost** triggers the alarm when contact with a device is lost, **Contact Established** triggers the alarm when contact is restored, and **Both** will trigger the alarm when contact is lost and when contact is regained.

### By Threshold

This option lets you define a threshold value that will be used to trigger the alarm. Click **Edit Threshold** and then refer to the [Edit Threshold Window](#) Help topic for information on defining threshold alarms. This option will be

disabled if your Management Center license does not include Management Center features that support threshold alarms (such as device statistics collection), and you do not have a Application Analytics license.


### By Flow

This option lets you open the [Edit Flow Criteria window](#) where you can define flow criteria that will be used to trigger the alarm. Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector.

### Device Groups

If desired, you can restrict the alarm to devices and port elements in one or more device groups. The alarm will only be raised on the devices and interfaces in the selected device groups. This allows you to filter alarms to specific devices or important ports. Use the **Select Groups** button to select the desired groups. Use the **Clear Group** button to remove the selected groups.

### *Actions Subtab*

Select the action that is performed when the alarm is triggered, and specify an alarm action limit, if desired. You can test an alarm action by clicking the Test Action button . (An alarm must be saved before it can be tested.)

### Email

Select this checkbox if you want an email sent if the alarm is triggered. Use the drop-down menu to select one of your pre-defined email lists. If no lists have been defined, the menu will be empty and you can click the Edit Email Lists button to define a list. There are default formats for the subject and body of the email, which can be overridden by selecting the Override Content checkbox.

### Syslog Server

Select this checkbox if you want to create a syslog message if the alarm is triggered. Enter the IP address or hostname that identifies the syslog server where the message will be sent. There is a default format for the syslog message sent to the server, which can be overridden by selecting the Override Content checkbox.

### Trap Server

Select this checkbox if you want to send an SNMP trap if the alarm is triggered. Enter the IP address for a trap receiver where the trap will be sent. Valid trap receivers are systems running an SNMP Trap Service. From the

Credential drop-down list select the appropriate SNMP credential that will be used when sending the trap to the trap receiver. Credentials are defined in the Profiles/Credentials tab in the Authorization/Device Access window (Tools > Authorization/Device Access). There is a default format for the trap message, which can be overridden by selecting the Override Content checkbox.

### isaac Service

Select this checkbox if you want to send a message to the isaac service if the alarm is triggered. The default alarm message is sent, or you can customize the message using the Override Content window. When you enable the isaac service action, it is seen as a notification in the Notifications panel in isaac. Then, when the alarm is triggered, a message is sent to isaac, and isaac forwards out the notification to alert isaac users. There is a default format for the isaac message, which can be overridden by selecting the Override Content checkbox.

### Program

Select this checkbox to specify a custom program or script that will be run on the Management Center Server if the alarm is triggered. In the Program field, enter the name of the program or use the **Select** button to open a file browser window and choose a program. In the Working Directory field, enter the path to the directory from which the program will be executed or use the **Select** button to open a file browser window and choose a directory. Any path references within your program that are not absolute paths, will be relative to the working directory. There is a default set of arguments passed to the program, which can be overridden by selecting the Override Content checkbox.

### Override Content

Select this checkbox if you want to override the default content contained in the action message or action program arguments. The default content is defined in the Console Alarms option (Tools > Options > Console > Alarms). Use the **Edit Content** button to open the [Edit Action Overrides window](#) where you can change the defaults for this specific notification only.

### Enable Action Limit

This option allows you to rate-limit the alarm actions by specifying a maximum number of times an action can be taken, and (optionally) a period of time after which actions can resume.

When this option is enabled, the Max Count determines the number of times an action will be performed for this alarm. Once the limit is reached, the alarm will still be recorded, but no further actions are performed. If you have

configured multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. If Enable Action Limit is not checked, there is no limit placed on the number of times the action will be performed.

If you specify a reset interval, then once that interval expires, the count is reset and actions will be executed until the Max Count is reached again. If the reset interval is set to "None", then once the alarm limit is reached, the alarm will not reset unless manually reset. You can reset the action counters for all current alarms related to this alarm definition using the **Reset All** button. For example, if there is a Flow Limit Alarm on three devices, it will reset the limits on those three alarms.

### *Other Options Subtab*

Select the desired option for how alarms will be cleared. All alarms can always be cleared manually.

#### **No Current Alarm (Action Only)**

When this option is selected, the Alarms Manager will only perform the configured actions, but will not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source will not change, and no alarm will be added to the system.

#### **Cleared by Alarms**

This option allows you to select the alarm(s) that will be used to clear the alarm you are defining. You must first create the alarm definitions for the clearing alarms, which must have the alarm severity set to "Clear". The clearing alarms should be triggered when the problem or condition is removed. Then, use the **Select Alarms** button to open a window where you can select one or more clearing alarms that will clear the alarm you are defining.

#### **New Alarm Button**

Opens a window where you can enter a name for a new alarm.

#### **Delete Alarm Button**

Removes the alarm you have selected in the table. When an alarm is deleted, its current alarms are also deleted. You must click **Apply** or **OK** for the delete to take effect.

#### **Rename Alarm Button**

Opens a window where you can change the name of the alarm you have selected in the table. You must click **Apply** or **OK** for your change to take effect.



### **Set Mail Config Button**

Opens the SMTP E-Mail Server Options window where you can define your outgoing e-mail server and the sender's address for your e-mail notifications.

### **Disable Alarms Button**

Allows you to disable all alarms. For example, you might want to temporarily disable alarms while you are performing network maintenance. When you disable alarms, the alarm events that trigger or clear alarms will be ignored, and no alarm actions will be performed.

### **Restore Default Alarms**

Restores any default alarm definitions that have been deleted. Any existing default alarms will not be overwritten.

### **OK/Apply Button**

After you add, edit, or delete an alarm definition, you must click **Apply** or **OK** for your changes to take effect.

---

## **Related Information**

For information on related windows:


- [Edit Action Overrides Window](#)
- [Edit Custom Alarm Criteria Window](#)
- [Trap Selection Window](#)


For information on related tasks:


- [How to Configure Alarms](#)
- [How to Configure Custom Alarm Criteria](#)

## Basic Policy Tab (Default Port Role View)

---

The **Basic Policy** Tab (Default Port Role view) displays the default policy role configured for each port and lets you change the role, if desired. To access the tab, select one or more devices or device groups in the left-panel tree, and click the **Basic Policy** tab in the right panel. Select the **Default Port Role** option at the top of the tab. The tab displays a table of port information for all the selected devices. The **Table Editor** button  activates the editing row where you can change a port's alias and default policy role.

**IMPORTANT:** The **Basic Policy** tab is not automatically updated. Instead, the tab must be refreshed using the  (Retrieve button) to update the table information each time you access this tab. The first time you access the **Basic Policy** tab, the table is blank making it necessary to click Retrieve to display port information. If you leave the **Basic Policy** tab and then return, the content of the table will not have changed, even though conditions on device ports may have changed. You must again retrieve the information for current data.

Use the table options and tools to find, filter, sort, print, and export information in the table and customize table settings. You can access the Table Tools 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). For more information, see the Table Tools Help topic.

IP Address	Display Name	Slot	Port	Name	Description	Alias	Default
10.20.10.25	10.20.10.25	2	21010	fe.2.10	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21011	fe.2.11	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21012	fe.2.12	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21013	fe.2.13	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21014	fe.2.14	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21015	fe.2.15	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21016	fe.2.16	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21017	fe.2.17	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21018	fe.2.18	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21019	fe.2.19	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21020	fe.2.20	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21021	fe.2.21	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21022	fe.2.22	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21023	fe.2.23	Enterasys Networks,...		Administrator
10.20.10.25	10.20.10.25	2	21024	fe.2.24	Enterasys Networks,...	ID345	Enterprise User
10.20.10.25	10.20.10.25	2	21025	fe.2.25	Enterasys Networks,...		<None>
10.20.10.25	10.20.10.25	2	21026	fe.2.26	Enterasys Networks,...		<None>

### IP Address

The IP address of the device and the SNMP Context (when applicable).

### Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

### Slot

The range of ports in some devices span multiple slots. For these devices, this column shows the board location (slot) within the chassis where the port is located.

### Port

The port number (ifIndex).

### Name

The port interface name.

### Description

A description of the port.







## Alias

The alias (ifAlias) for the interface. You can create a port alias to help identify that port based on your network configuration. You can add or change the alias for a port using the [Table Editor](#).

## Default Role

The default role configured for the port. A port's default role takes effect when an end user on a port fails to authenticate, or if authentication is inactive on the port. You can change the default role for a port using the [Table Editor](#).

## Table Editor

Use the Table Editor to change the alias and/or default role of a port. Select one or more ports in the table, and click the **Table Editor** button . The Table Editor row appears at the bottom of the table. You can enter an alias in the Alias column. The Default Role column has a drop-down list that displays the roles that have been enforced to the selected devices where the ports are located. (If you have selected ports from multiple devices, the list displays only those roles that the devices have in common.) Once you enter an alias and/or select a new role, a green exclamation mark  indicates the ports that have been changed (but not Applied) and the **Apply** button  becomes active. Clicking the **Table Editor** button  at this point cancels your changes, restores the original values, and hides the Table Editor. Clicking the **Apply** button  sets the values that you've changed for the selected ports, removes the , and hides the Table Editor row.

### **Table Editor Button**

Toggles the Table Editor row, where you can change a port's alias and default role.

### **Apply Button**

Sets any values that you've changed on the ports.

### **Retrieve Button**

Contacts the selected devices or device groups to update the table information. While retrieving information, the button changes to a red octagon.

---

## Related Information

For information on related windows:


- [Basic Policy Tab \(End User Sessions View\)](#)


## Basic Policy Tab (End User Sessions View)

---

The **Basic Policy** Tab (End User Sessions view) displays port end user sessions. To access the tab, select one or more devices or device groups in the left-panel tree, and click the **Basic Policy** tab in the right panel. Select the End User Sessions option at the top of the tab to display information about each login session for the ports on the selected devices, including the current values being collected for a session still in progress, or the final values for the last valid session when there is no session currently active. For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port (such as the RoamAbout R2 and the Matrix N-Series Platinum devices), all users authenticated on its ports will be listed in the table, along with the roles under which they are authenticated.

The [Results Filter](#) right-click menu option lets you select the result categories that appear in the table (802.1x, MAC, Web-based, etc.). When the **Active Sessions** checkbox is checked in the Results filter, only your active sessions are displayed.

**IMPORTANT:** The **Basic Policy** tab is not automatically updated. Instead, the tab must be refreshed using the  (Retrieve button) to update the table information each time you access this tab. The first time you access the **Basic Policy** tab, the table is blank making it necessary to click retrieve to display port information. If you leave the **Basic Policy** tab and then return, the content of the table will not have changed, even though conditions on device ports may have changed. You must again retrieve the information.

Use the table options and tools to find, filter, sort, print, and export information in the table and customize table settings. You can access the Table Tools 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). For more information, see the Table Tools Help topic.

The screenshot shows the 'Basic Policy' tab with the 'End User Sessions' view selected. The 'Results Filter' section is active, showing the following options:  802.1X,  MAC,  Web-Based,  CEP,  Active Sessions,  Row Count,  VLAN, and  Statistics. The table below displays 18 rows of session data.

	IP Address	Display Name	Slot	Port	Name	Description	Alias	State	Current R
1	10.20.77.36	10.20.77.36	1	12001	ge.1.1	Enterasys Netw...		Un-authentica...	<Unknown>
2	10.20.77.36	10.20.77.36	1	12001	ge.1.1	Enterasys Netw...		Un-authentica...	<Unknown>
3	10.20.77.36	10.20.77.36	1	12002	ge.1.2	Enterasys Netw...		Un-authentica...	<Unknown>
4	10.20.77.36	10.20.77.36	1	12002	ge.1.2	Enterasys Netw...		Un-authentica...	<Unknown>
5	10.20.77.36	10.20.77.36	1	12003	ge.1.3	Enterasys Netw...		Un-authentica...	<Unknown>
6	10.20.77.36	10.20.77.36	1	12003	ge.1.3	Enterasys Netw...		Un-authentica...	<Unknown>
7	10.20.77.36	10.20.77.36	1	12004	ge.1.4	Enterasys Netw...		Un-authentica...	<Unknown>
8	10.20.77.36	10.20.77.36	1	12004	ge.1.4	Enterasys Netw...		Un-authentica...	<Unknown>
9	10.20.77.36	10.20.77.36	1	12005	ge.1.5	Enterasys Netw...		Un-authentica...	<Unknown>
10	10.20.77.36	10.20.77.36	1	12005	ge.1.5	Enterasys Netw...		Un-authentica...	<Unknown>
11	10.20.77.36	10.20.77.36	1	12006	ge.1.6	Enterasys Netw...		Un-authentica...	<Unknown>
12	10.20.77.36	10.20.77.36	1	12006	ge.1.6	Enterasys Netw...		Un-authentica...	<Unknown>
13	10.20.77.36	10.20.77.36	1	12007	ge.1.7	Enterasys Netw...		Un-authentica...	<Unknown>
14	10.20.77.36	10.20.77.36	1	12007	ge.1.7	Enterasys Netw...		Un-authentica...	<Unknown>
15	10.20.77.36	10.20.77.36	1	12008	ge.1.8	Enterasys Netw...		Un-authentica...	<Unknown>
16	10.20.77.36	10.20.77.36	1	12008	ge.1.8	Enterasys Netw...		Un-authentica...	<Unknown>
17	10.20.77.36	10.20.77.36	1	12009	ge.1.9	Enterasys Netw...		Un-authentica...	<Unknown>
128									

## Results Filter

The Results Filter is accessed through a right-mouse click on a column heading or anywhere in the table body. It lets you select the result categories that appear in the table:

- 802.1x - Show 802.1X authentication sessions
- MAC - Show MAC authentication sessions
- Web-Based - Show Web-Based (PWA) authentication sessions
- CEP - Show CEP authentication sessions
- Active Sessions - Show only active sessions
- Row Count - Show the row count column in the left-most column of the table
- VLAN - Display the following four columns in the table:
  - [Policy PVID Override Status](#)
  - [Policy PVID Override](#)
  - [VLAN ID](#)
  - [VLAN Oper Egress](#)

- Statistics - Display table columns that show received/transmitted bytes and received/transmitted frames during each session.

#### **IP Address**

The IP address of the device and the SNMP Context (when applicable).

#### **Display Name**

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

#### **Slot**

The range of ports in some devices span multiple slots. For these devices, this column shows the board location (slot) within the chassis where the port is located.

#### **Port**

The port number (ifIndex).

#### **Name**

The port interface name.

#### **Description**

A description of the port.

#### **Alias**

The alias (ifAlias) for the interface.

#### **State**

The end user's authentication status: a blue circle indicates an authenticated end user, a gray circle indicates an unauthenticated end user.

#### **Current Role**

The role under which the user authenticated on the port.

#### **Policy PVID Override Status**

Indicates whether default access control (a default VLAN) has been enabled for the current role. Default access control allows you to permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. The default VLAN overrides the 802.1Q PVID for the port. You must have the VLAN checkbox selected in the [Results Filter](#) to see this column.

#### **Policy PVID Override**

If default access control (a default VLAN) has been enabled for the current role and configured to contain traffic to a VLAN, this column displays the associated VLAN ID. The VLAN will be applied to all untagged frames



arriving on the port that do not match any VLAN traffic classification rules, and overrides the 802.1Q PVID for the port. A value of 0 indicates that the default access control is configured to drop all frames that do not match a classification rule (Deny Traffic). A value of 4095 indicates that the default access control is configured to forward any frames that do not match a classification rule (Permit) using the 802.1Q PVID. You must have the VLAN checkbox selected in the [Results Filter](#) to see this column.

#### **VLAN ID**

If the user authenticated via RFC 3580 VLAN Authorization, this is the VLAN ID that was returned from the RADIUS server. A VLAN ID value of 0 indicates that no VLAN was assigned. If VLAN authentication is not supported on the device, this column will display "N/A." You must have the VLAN checkbox selected in the [Results Filter](#) to see this column.

#### **VLAN Oper Egress**

The modification that will be made to the VLAN egress list for the VLAN ID returned by the RADIUS server, if the user authenticated via RFC 3580 VLAN Authorization.

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list.

If VLAN authentication is not supported on the device, this column will display "N/A." You must have the VLAN checkbox selected in the [Results Filter](#) to see this column.

#### **Type**

The authentication type of this login session: Web-Based, 802.1x, or MAC.

#### **IP Address**

The IP address of the remote user of this login session.

#### **MAC Address**

The MAC address of the remote user of this login session.

#### **Authentication Status**

On Matrix N-Series Platinum devices, the authentication status of the login session. All other devices will display "N/A." Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

### Terminate Cause

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

### User Name

The user name provided by the end user at login (authentication).

### Received Bytes

The number of bytes received in user data frames on this port during this session. You must have the Statistics checkbox selected in the [Results Filter](#) to see this column.

### Transmitted Bytes

The number of bytes transmitted in user data frames on this port during this session. You must have the Statistics checkbox selected in the [Results Filter](#) to see this column.

### Received Frames

The number of user data frames received on this port during this session. You must have the Statistics checkbox selected in the [Results Filter](#) to see this column.

### Transmitted Frames

The number of user data frames transmitted on this port during this session. You must have the Statistics checkbox selected in the [Results Filter](#) to see this column.

### Start Time

The time and date when the login session started.

### Duration

The duration of the login session, in the format D + HH:MM:SS.



### (Retrieve)

Contacts the selected devices or device groups to update the table information. While retrieving information, the button changes to a red octagon.

---

## Related Information

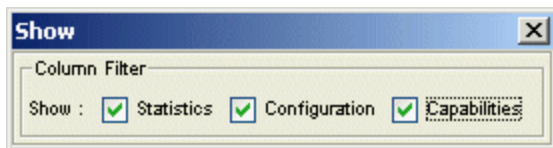
For information on related windows:

- [Basic Policy Tab \(Default Port Role View\)](#)

## Column Filter Toolbar

---

The Column Filter Toolbar lets you select the information is presented in the [Ports - Properties Tab](#). The toolbar is active, by default when the Ports - Properties tab is selected in the right panel. You control access to the Column Filter toolbar by right-clicking on a column header or anywhere in the body of the table and selecting **Column Filter** from the popup menu. 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. You can also click and drag the toolbar into a separate window as shown here.



### Statistics

When selected, the following columns showing port traffic statistics appear in the table:

- In Octets
- In Ucast Pkts
- In Discards
- In Errors
- In Unknown Packets
- Out Octets
- Out Ucast Pkts
- Out Discards
- Out Errors
- Out Unknown Packets

### Configuration

When selected, the following columns, used to configure auto negotiation for selected port(s), appear in the table:

- Remote Auto Signal
- Auto Negotiate Configuration
- Auto Negotiate Mode

- Speed (Current)
- Speed (Manual)
- Duplex Mode (Current)
- Duplex Mode (Manual)
- Flow Control (Current)
- Flow Control (Manual)

### Capabilities

When selected, the following columns showing the operational modes and advertised modes appear in the table:

- [Advertised Capabilities](#)
- 

### Related Information

For information on related windows:

- [Port - Properties Tab](#)

## Compass Tab

---

Compass is a powerful search tool that provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations. You can use Compass to search one or more devices or device groups selected in the Console left panel. The search is based on the following:

- the selection you make in the Console left panel ([Search Scope](#))
- the [Search Type](#) you select on the Compass tab
- the [Search Parameters](#) you provide on the Compass tab

The bottom section of the Compass tab provides two tabs, one for viewing a log of the search process ([Search Log tab](#)), and the other for the search results ([Results tab](#)). (If this bottom section of the tab is not visible, click the panel control up button ▲ at the foot of the tab.)

To access the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel.

### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel. The selected search scope is displayed at the top of the tab.

**Note:** If you do a search on a user-defined device group that contains interfaces, the whole device on which the interface is located will be searched.

### Search Type

Select the type of search you want to perform from the drop-down list. For more information on the different types of searches, see the following links:

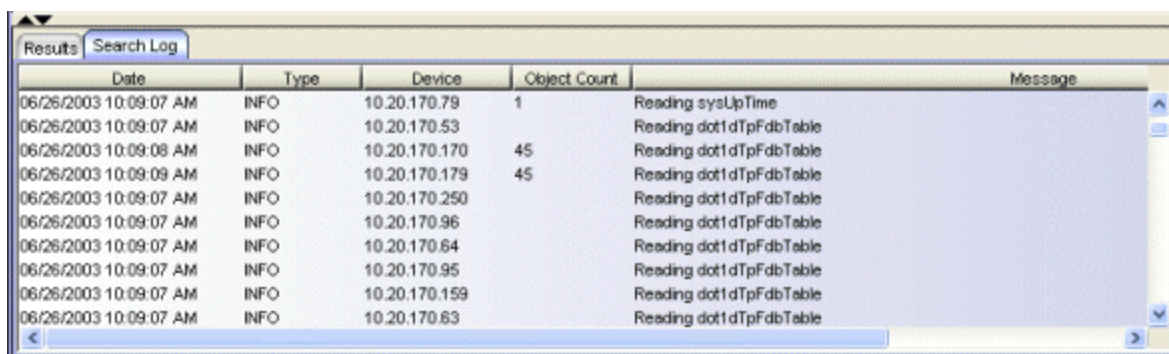
- [All](#)
- [Auto](#)
- [IP Address](#)
- [IP Subnet](#)
- [MAC Address](#)
- [Multicast Address](#)
- [User Name](#)

## Search Parameters

If you provide specific search parameters, Compass returns information on those parameters, if it finds them within the search scope. If you do not provide specific search parameters, Compass returns information on everything within the search scope.

## Search Log Tab

This tab displays a log of the progress of the search and notifies you of unsupported devices. You can customize table settings and find, filter, sort, print, and export the information in the Search log. Access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.



Date	Type	Device	Object Count	Message
06/26/2003 10:09:07 AM	INFO	10.20.170.79	1	Reading sysUpTime
06/26/2003 10:09:07 AM	INFO	10.20.170.53		Reading dot1dTpFdbTable
06/26/2003 10:09:08 AM	INFO	10.20.170.170	45	Reading dot1dTpFdbTable
06/26/2003 10:09:09 AM	INFO	10.20.170.179	45	Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.250		Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.96		Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.64		Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.95		Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.159		Reading dot1dTpFdbTable
06/26/2003 10:09:07 AM	INFO	10.20.170.63		Reading dot1dTpFdbTable

### Date

Date and time the search was performed.

### Type

Message type, e.g. INFO (informational), ERROR, WARNING.

### Device

IP address of the device queried.

### Object Count

The number of responses for objects found by the search.

### Message

Describes the specific action performed by the search.


## Results Tab

This tab displays the results of the Compass search in table form. For column definitions and specific information on the Results tab beyond that given below,

see the links for the different [search types](#).

### *Right-click Menu*

You can customize table settings and find, filter, sort, print, and export the information in the Search log. Access these Table Tools through a right mouse click on a column heading or anywhere in the table body. You can also utilize the following right-click menu options in the table:

- **Results Filter** - This toolbar provides filtering options for the Results table. All the options except **CDP/Backplane/Host Data Ports**, **Duplicate MAC**, **Duplicate IP**, and **Collapsed** are checked by default. You can select the view options before or after the search is completed. When the window is too narrow to display all of the Results Filter options, the  button appears at the right side of the tool bar. Clicking this button provides access to the hidden options. To close the Results Filter toolbar, click the red X.
- **Show Layer 2** - Layer 2 entries will be displayed in the table.
- **Show Layer 3** - Layer 3 entries will be displayed in the table.
- **Show Layer 4** - Layer 4 entries will be displayed in the table.
- **Show 10/100 Mb Only** - Only entries for 10/100 Mb ports will be displayed in the table.
- **Show CDP/Backplane/Host Data Ports** - CDP, backplane, and host data ports will be displayed in the table.
- **Show Duplicate MAC** - Duplicate MAC Addresses will be displayed in the table.
- **Show Duplicate IP** - Duplicate IP Addresses will be displayed in the table.
- **Show Collapsed** - Entries with duplicate information will be displayed only once in the table.
- **Go To View > Device Properties** - Opens the [Properties tab](#) for the selected device.
- **Go To View > Port Properties** - Opens the [Properties tab](#) for the selected port.
- **Port Tools > Port Monitor** - Opens the [Port Monitor window](#) for the selected port.
- **Port Tools > Interface Statistics** - Opens the Interface Statistics window for the selected port.



- **Port Tools > RMON Ethernet Statistics** - Opens the RMON Ethernet Statistics window for the selected port.
- **Port Tools > RMON History List** - Opens the RMON History List window for the selected port.
- **Add Devices to Group** - Opens the [Add Device\(s\) to a Group window](#), where you can add the selected device(s) to a group.
- **Select All** - Selects all the entries in the table.

### *User Location Information*

You can get an indication of the location of a user by viewing the Active column in the Results tab. This column indicates entries that come from the *dot1dTp*, *dot1x* and **etsysPwa** MIBs. These MIBs give the best indication of an end station's actual location. Entries in the *dot1Tp* MIB are automatically added and deleted based on when they were last heard. If an end station address has not been heard for more than 5 minutes, it is deleted. On the other hand, the *ctAliasTable* never removes entries automatically; instead, it requires a manual step. Therefore, if the end station moves, the entry is never removed from the table and may give a false impression of the end station's true location.

### **Search Button**

Initiates the search based on the criteria you provide. The button changes to **Stop** after you initiate the search, and you can stop the search at any time by clicking **Stop**. If the search seems to take longer than expected, it is most likely because a network element or elements cannot be contacted. In this case, a message indicating that there were errors during the search is displayed. You can either bypass the message to complete the search, or elect to view the Event Log.

## **Status Bar**

The status bar at the bottom of the NetSight Console window provides messages related to the status of the search, and a progress bar showing the percentage of the search completed.

---

### **Related Information**

For information on related tasks:

- [How to Use Compass](#)

For information on related windows:

- [Add Device\(s\) to Group window](#)
- [Compass Tab All Search](#)
- [Compass Tab Auto Search](#)
- [Compass Tab IP Address Search](#)
- [Compass Tab IP Subnet Search](#)
- [Compass Tab MAC Address Search](#)
- [Compass Tab Multicast Address Search](#)
- [Compass Tab User Name Search](#)
- [Ping Window](#)

## Compass Tab All Search

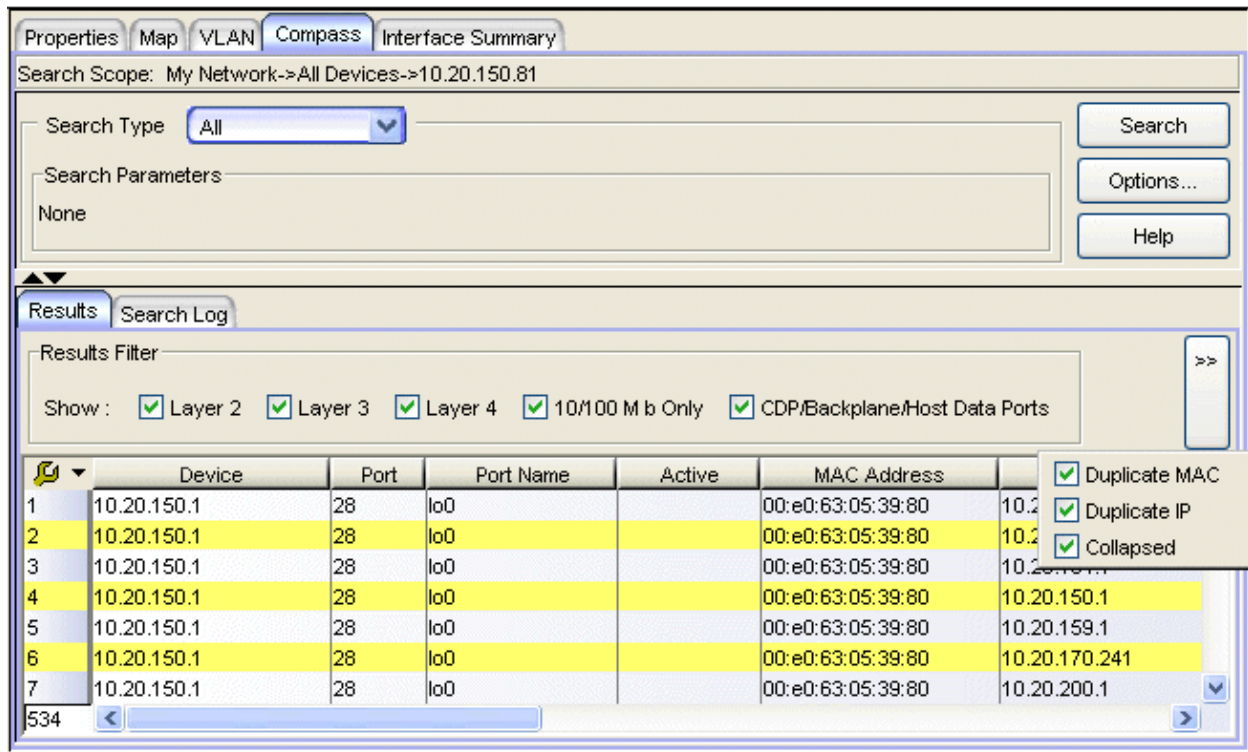
The All search on the [Compass tab](#) lets you collect and display address data for any device(s) or device group(s) selected in the left panel. Data is collected from all the MIBs that Compass has implemented. The following table lists the MIBs used to collect information for each column in the Results table.

Column	MIBs
<b>Port</b>	addressMap Table, ctAlias Table, ctIGMPCache Table, dot1dTpFdbPort Table, dot1qTpFdbPort Table, dot1xAuthSession Table, etsysDot1xAuthSession Table, etsysMACAuthenticationSession Table, etsysMACLockingStation Table, etsysPwaAuthSession Table, hostAddress Table, igmpCacheTable, ipNetToMediaPhysAddress Table
<b>Port Name</b>	ifName Table
<b>MAC</b>	addressMap Table, ctAlias Table, dot1dTpFdbPort Table, dot1qTpFdbPort Table, dot1xAuthSession Table, etsysDot1xAuthSessionStats Table, etsysMACAuthenticationSession Table, etsysMACLockingStation Table, etsysPwaAuthSession Table, hostAddress Table, ipNetToMediaPhysAddress Table
<b>Address</b>	addressMap Table, ctAlias Table, ctIGMPCache Table, igmpCacheTable, ipNetToMediaPhysAddress Table, etsysPwaAuthSession Table

Column	MIBs
<b>Address Type</b>	addressMap Table, ctAlias Table, dot1dTpFdbPort Table, dot1qTpFdbPort Table, dot1xAuthSession Table, etsysDot1xAuthSessionStats Table, etsysMACAuthenticationSession Table, etsysMACLockingStation Table, etsysPwaAuthSession Table, hostAddress Table, igmpCacheTable Table, ipNetToMediaPhysAddress Table
<b>User Name</b>	dot1xAuthSession Table, etsysDot1xAuthSessionStats Table, etsysPwaAuthSession Table
<b>State</b>	dot1xAuthSession Table, etsysDot1xAuthSessionStats Table, etsysMACAuthenticationSession Table, etsysMACLockingStation Table, etsysPwaAuthSession Table
<b>VLAN Name</b>	dot1qCurrent Table, dot1qVlanStatic Table
<b>VLAN ID</b>	ctAlias Table
<b>Filter ID</b>	ctAlias Table, dot1qTpFdbPort
<b>Create Time</b>	ctAlias Table, dot1xAuthSession Table, etsysDot1xAuthSession Table, etsysMACAuthenticationSession Table, etsysPwaAuthSession Table
<b>Multicast Group</b>	ctIGMPCache Table, igmpCacheTable

The All search is similar to the MAC address search, except that it does not use a search parameter. If you need to filter the address data, use one of the specific Compass searches, or the Auto search.

To access the All search on the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the All Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.



### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the All search type from the drop-down list.

### Search Parameters

No search parameters are needed for the All search. To initiate the search, make sure the All search type is selected, and click **Search**. You can stop the search at any time by clicking the **Stop** button.

### Search Log Tab

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

### Results Tab

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu

options offered on this tab.

### Device

This column lists any network element which is aware of the device(s) in the search scope selected in the left panel. For example, the network element associated with the device may be connected to the device, or it may have contacted the device, or the device may be on the path to a device the network element contacted.

### Port

Port number of the port on the device.

### Active

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

### MAC Address

MAC address of the device.

### Address

Address (IP, UDP, etc.) of the network element. The next column (Address Type) tells you what type of address this is.

### Address Type

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

### Host Name

Host name associated with the network element's IP address, if applicable.

### User Name

User ID associated with the network element, if applicable.

### State

Current operating state of the network element. Possible values are:

State	Meaning
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive

<b>State</b>	<b>Meaning</b>
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed for the network element.

**Related Information**

For information on related tasks:

- [Searching All](#)

For information on related windows:

- [Compass Tab](#)

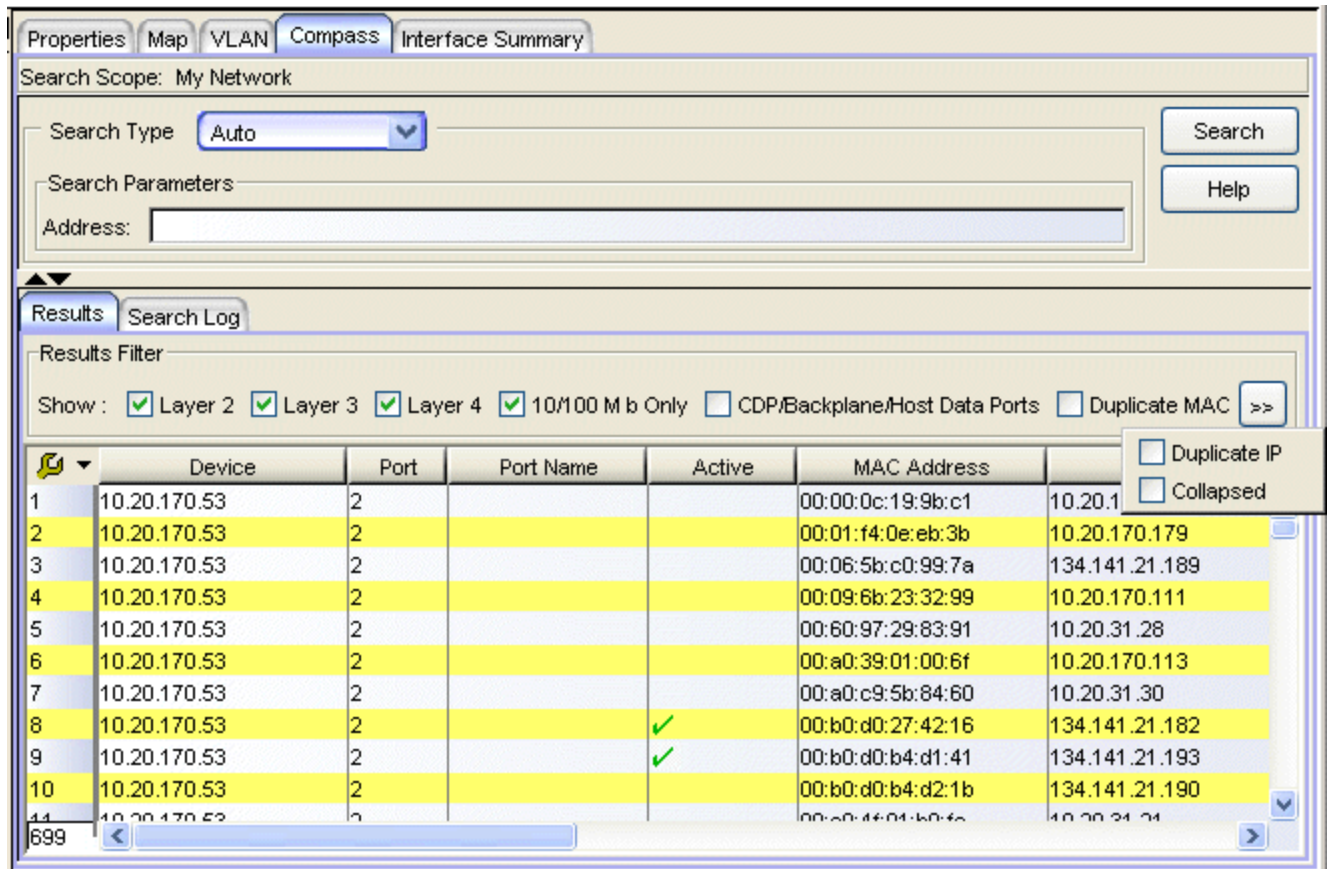
## Compass Tab Auto Search

---

The Auto search on the [Compass tab](#) auto-detects the address format you enter in the Search Parameters field, and performs the appropriate search on the device(s) or device group(s) selected in the left panel. For example:

- If you enter six bytes in hexadecimal format as a search parameter, Compass assumes it is a MAC address and performs a [MAC address search](#).
- If you enter four decimal bytes separated by periods, Compass assumes it is an IP address. If the IP address is a Multicast address it performs a [Multicast search](#); otherwise, it performs an [IP Address search](#). If the address contains a '/', with an IP address followed by a mask, it will do an [IP Subnet search](#).
- If the address entered is not a MAC address or an IP address, Compass attempts to resolve the entry to a hostname first and then a nickname, and if it succeeds, performs an IP address search. If the entry is not a hostname or nickname, MAC address or IP address, Compass performs a [User Name search](#).
- If you don't enter a search parameter, the Auto search performs an [All search](#).

To access the Auto search on the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the Auto Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.



### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the Auto search type from the drop-down list.

### Search Parameters

Enter a search parameter in the Address text box. If you don't enter a search parameter, Auto search performs an [All](#) search. Compass performs the search within the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

### Address

Enter the address, hostname, or nickname on which you want to search. Examples of the allowed formats are listed below. Compass will determine what type of entry it is, and perform the search for the entry within the selected [scope](#) of network elements.



- **MAC Address**
  - 00001dabcdef
  - 0.0.1d.ab.cd.ef
  - 0 0 1d ab cd ef
  - 0-0-1d-ab-cd-ef
  - 0:0:1d:ab:cd:ef
- **IP Address**
  - 1.2.3.4
- **IP Subnet**
  - 1.2.3.4/16
  - 1.2.3.4/255.255.0.0
- **Hostname, Nickname, or Username**
  - red

### *Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

### *Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu options offered on this tab.

#### **Device**

This column lists any device within the selected search scope which is aware of the address or hostname specified as the search parameter. For example, the network element associated with the search parameter may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

#### **Port**

Port number of the port which is aware of the network element's address or hostname. The network element may be connected to this port.

#### **Port Name**

Port name of the port which is aware of the network element's address or hostname. The network element may be connected to this port.

**Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

**MAC Address**

MAC address of the network element associated with the address or hostname.

**Address**

Address (IP, UDP, etc.) of the network element. The next field (Address Type) tells you what type of address this is.

**Address Type**

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

**Host Name**

Host name associated with the network element's IP address, if applicable.

**User Name**

User ID associated with the network element, if applicable.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.
connecting	connection in process

---

State	Meaning
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed on this line of the table.

---

**Related Information**

For information on related tasks:

- [Auto Searching](#)

For information on related windows:

- [Compass Tab](#)

## Compass Tab

### IP Address Search

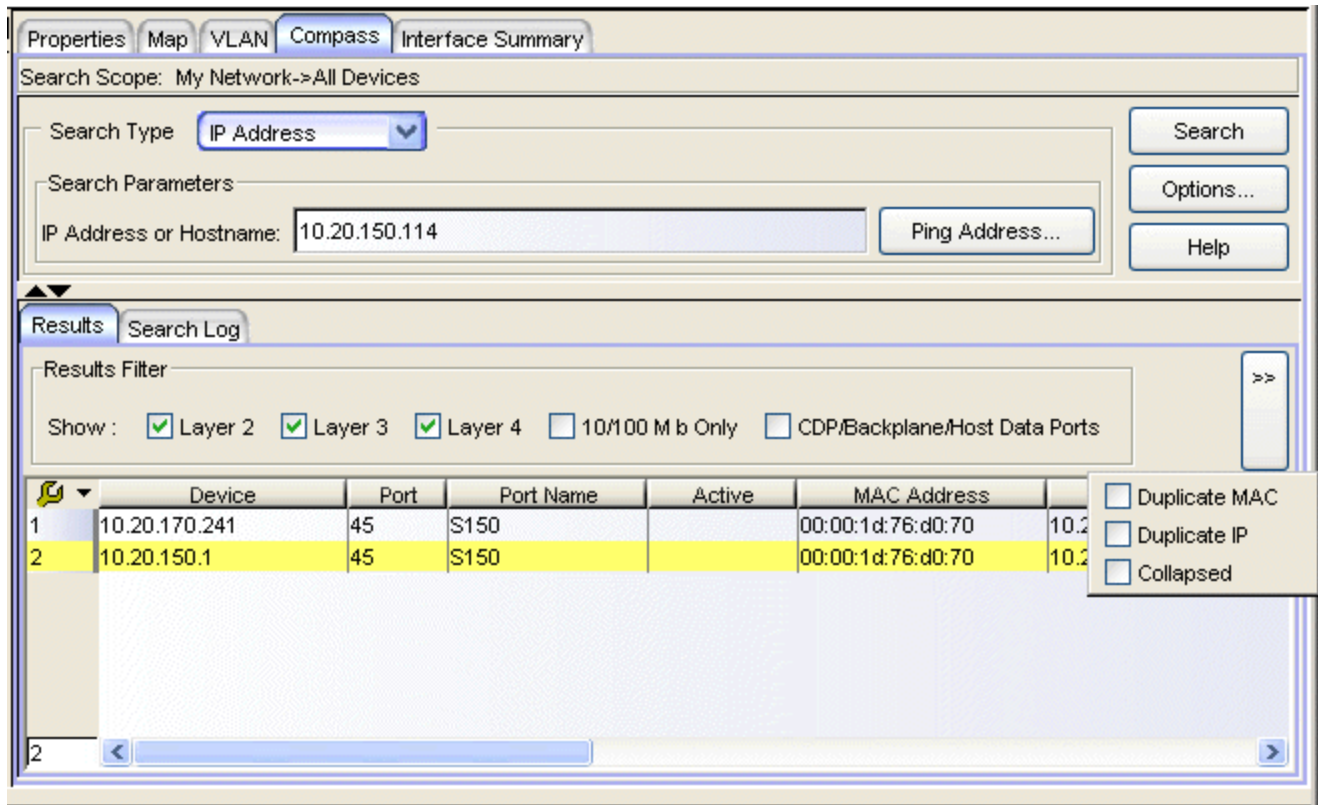
---

The IP address search on the [Compass tab](#) lets you search any device(s) or device group(s) selected in the left panel for an IP address. You can search for a specific IP address/hostname or for all IP addresses (including multicast addresses). Search results list any device which is aware of the specified IP address. For example, the network element associated with the specified IP address may be connected to the device, or it may have contacted the device, or the device may be on the path to a device the network element contacted. For Layer 2 devices, the IP address search will attempt to use information from a router within the search scope to locate an IP address. The IP address search looks at the following tables:

- ctAliasTable
- ctCDPNeighbor
- ctIfTable
- ctIGMP MIB
- dot1qVlanCurrentTable
- dot1qVlanStaticTable
- etsysPwaAuthPwaState
- etsysPwaAuthSessionStatsTable
- ifTable
- igmpCache
- ipNetToMediaTable
- sysUpTime
- RMON2 addressMap
- dot1qTpFdbPort
- dot1dTpFdbPort
- dot1dBasePortTable
- ipCidrRouteTable
- dot1xAuthSessionStatsTable
- etsysdot1xAuthSessionStatsTable
- RMONHostControlTable
- etsysMacAuthSessionTable
- etsysMultiAuthSessionStationTable
- MacLockingStationTable
- etsysConvEndPointConnMac
- IfXtable

To access the IP address search on the Compass tab, select the desired device (s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the IP Address Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.

The Compass IP address search tab also provides the ability to ping an IP address.



### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the IP Address search type from the drop-down list.

### Ping Address Button

Opens the [Ping window](#), where you can ping the network element associated with a specific IP address. If you have already entered an IP address on the Compass tab, that IP address will be pre-entered in the Ping window.

### Search Parameters

Compass performs the search on the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To search for information on a specific IP address or hostname, enter it in the IP Address or Hostname text box. If you leave the IP Address or Hostname text field blank, Compass will search for all IP addresses within the scope. To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

**IP Address or Hostname**

Enter the specific IP address or hostname on which you want to search. You can also search by device nickname, if desired. (This field does not accept any spaces, so if the device nickname has spaces in it, use the [Auto search](#) instead.)

*Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

*Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu options offered on this tab.

**Device**

This column lists any device within the selected scope which is aware of the specified IP address/hostname. For example, the network element associated with the IP address may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

**Port**

Port number of the port which is aware of the network element's IP address/hostname. The network element may be connected to this port.

**Port Name**

Port name of the port which is aware of the network element's IP address/hostname. The network element may be connected to this port.

**Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

**MAC Address**

MAC address of the network element associated with the IP address.

**Address**

IP Address of the network element. If you searched on a specific IP address, this is where that address is displayed.

**Address Type**

Type of address displayed in the Address field, in this case "IP".

**Host Name**

Host name associated with the network element's IP address, if applicable.

**User Name**

User ID associated with the network element, if applicable.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed on this row of the table.

---

**Related Information**

For information on related tasks:

- [Searching IP Addresses](#)

For information on related windows:

- [Compass Tab](#)
- [Ping Window](#)

## Compass Tab

### IP Subnet Search

---

The IP subnet search on the [Compass tab](#) enables you to search for the members of a specified subnet (including multicast addresses) within the device (s) or device group(s) selected in the left panel. The IP subnet search looks at the following tables:



- ctAliasTable
- ctCDPNeighbor
- ctIfTable
- ctIGMP MIB
- dot1dTpFdTable
- dot1qTpFdTable
- dot1qVlanCurrentTable
- dot1qVlanStaticTable
- etsysConvEndPointConnMacTable
- etsysPwaAuthPwaState
- etsysPwaAuthSessionStatsTable
- ifTable
- ifXtable
- igmpCache
- ipNetToMediaTable
- RMON2 addressMap
- sysUpTime

To access the IP Subnet search on the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the IP Subnet Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.

The screenshot shows the Compass tab interface with the following details:

- Search Scope:** My Network->All Devices
- Search Type:** IP Subnet
- Search Parameters:**
  - IP Address: 10.20.150.1
  - Subnet Mask: 24 (example: 16)
- Buttons:** Search, Options..., Help
- Results Filter:**
  - Show:  Layer 2,  Layer 3,  Layer 4,  10/100 M b Only,  CDP/Backplane/Host Data Ports
- Results Table:**

	Device	Port	Port Name	Active	MAC Address	
1	10.20.150.130	1	XMIB2_NAME_STR		00:e0:63:05:39:80	10.20.150.130
2	10.20.150.1	28	lo0		00:e0:63:05:39:80	10.20.150.1
3	10.20.150.76	77			00:e0:63:05:39:80	10.20.150.76
4	10.20.150.76	77			00:e0:63:05:39:80	10.20.150.1
5	10.20.170.241	28	lo0		00:e0:63:05:39:80	10.20.150.1
- Filters:**
  - Duplicate MAC
  - Duplicate IP
  - Collapsed

### Search Scope

The scope within which the search will be performed, based on the device(s) or device group(s) selected in the left panel.

## Search Type

Select the IP Subnet search type from the drop-down list.

## *Search Parameters*

Compass performs the search on the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To search for the members of a subnet within the scope selected in the left panel, enter an IP address from the subnet in the IP Address text field, and enter a network mask value which defines the subnet group. To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

## IP Address

Enter an IP address from the subnet you want to search. Compass will look for the members of the subnet within the selected [scope](#).

## Subnet Mask

When you click this text box, it defaults to the natural network mask value, unless you enter a different one. The format of this text box depends on the format selected for the Suite-Wide Data Display Network Mask option in the **Tools > Options** window: either CIDR or dot-delimited. An example of the selected format is provided below the text box.

## *Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

## *Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for the table capabilities, and the other right-click menu options offered on this tab.

## Device

This column lists any device which is aware of the IP subnet. For example, the network element associated with the IP subnet may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

## Port

Port number of the port which is aware of the network element's IP subnet. The network element may be connected to this port.

**Port Name**

Port name of the port which is aware of the network element's IP subnet. The network element may be connected to this port.

**Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

**MAC Address**

MAC address of the network element associated with the IP subnet.

**Address**

Address (IP, UDP, etc.) of the network element. The next field (Address Type) tells you what type of address this is.

**Address Type**

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

**Host Name**

Host name associated with the network element's IP address, if applicable.

**User Name**

User ID associated with the network element, if applicable.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.

---

State	Meaning
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed on this line of the table.

---

**Related Information**

For information on related tasks:

- [Searching IP Subnets](#)

For information on related windows:

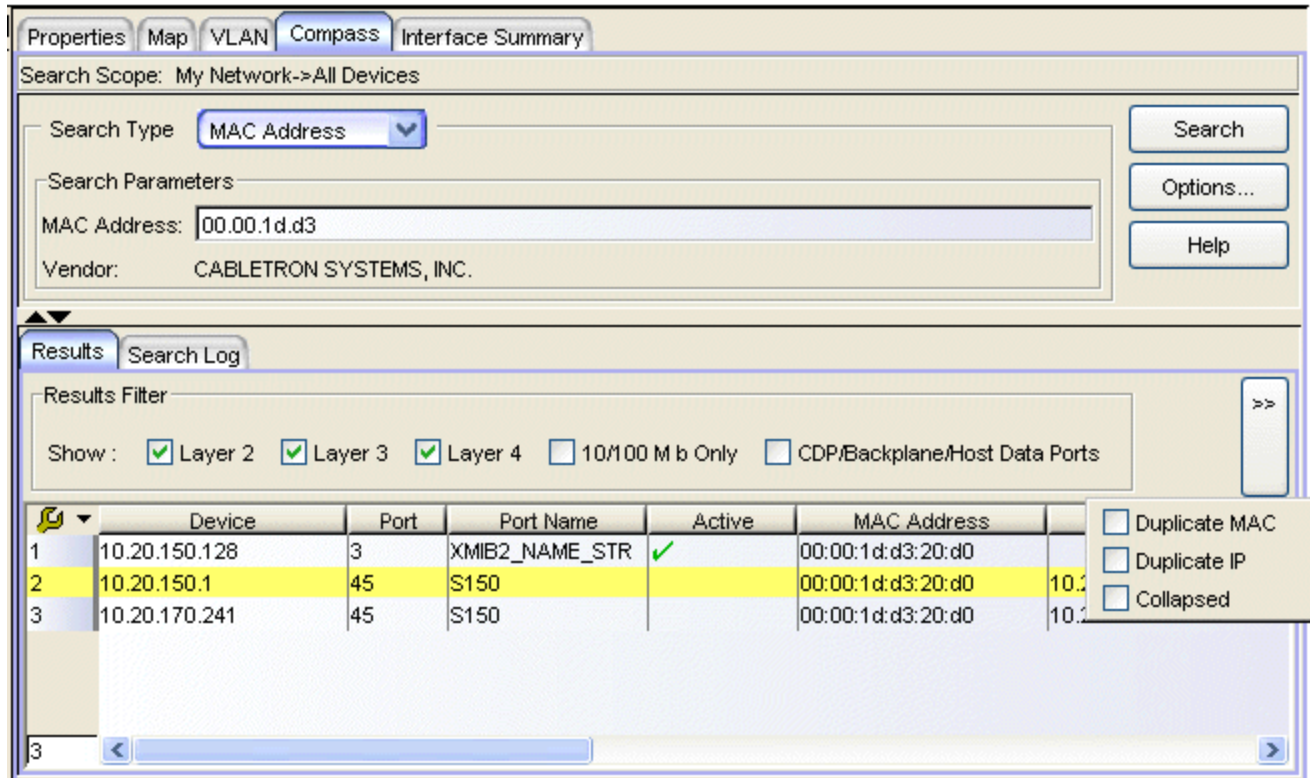
- [Compass Tab](#)

## Compass Tab MAC Address Search

The MAC address search on the [Compass tab](#) lets you search any device(s) or device group(s) selected in the left panel for a MAC address. You can search for a specific MAC address, a partial MAC address (for example, to find all of a specific vendor's equipment), or on all of the selected network elements. The MAC address search looks at the following tables:

- ctAliasTable
- ctCDPNeighbor
- ctIfTable
- dot1dBasePortTable
- dot1dTpFdbTable
- dot1qTpFdbTable
- dot1qVlanCurrentTable
- dot1qVlanStaticTable
- dot1xAuthPaeState
- dot1xAuthSessionStatsTable
- etsysConvEndPointMacTable
- etsysDot1xAuthSessionStatsTable
- etsysMACAuthenticationSessionTable
- etsysMACLockingStationTable
- etsysMultiAuthSessionStationTable
- etsysPwaAuthPwaState
- etsysPwaAuthSessionStatsTable
- ifTable
- ipNetToMediaTable
- RMON hostControlTable
- RMON2 addressMap
- sysUpTime

To access the MAC address search on the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the MAC Address Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.



### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the MAC Address search type from the drop-down list.

### Search Parameters

Compass performs the search on the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To search for information on a specific MAC address, enter it in the MAC Address text field. To do a partial MAC address search (for example, if you want to search for a specific vendor's equipment within the selected scope), enter enough of the address in the MAC Address text box to identify the vendor. If you leave the MAC Address text field blank, Compass will search for all MAC addresses within the scope. To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

**NOTE:** Because IGMP does not return MAC addresses, using the non-filtered MAC address search may not return all the addresses associated with the devices in the scope. To do a complete search for all addresses, use the [All search](#).

## MAC Address

Enter the specific MAC address for which you want to search. Compass will look for this address within the selected search scope. You can also enter a partial address, to search for a specific vendor's equipment (e.g. 0 . 0 . 1d). (See <http://standards.ieee.org/regauth/oui/oui.txt> for vendor MAC address prefixes.) Formats allowed are dot, colon, space, dash, and no delimiter:

- 0 . 0 . 1d . 1 . 2 . 3
- 00 : 00 : 1D : 01 : 02 : 03
- 00 00 1D 01 02 03
- 00-00-1D-01-02-03
- 00001D010203

## Vendor

The vendor for the hardware associated with the MAC address you are entering appears here as soon as you type enough of the MAC address for Compass to recognize it.

## *Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

## *Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu options offered on this tab.

## Device

This column lists any device within the selected scope which is aware of the specified MAC address. For example, the network element associated with the MAC address may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

## Port

Port number of the port which is aware of the network element's MAC address. The network element may be connected to this port.

## Port Name

Port name of the port which is aware of the network element's MAC address. The network element may be connected to this port.

**Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

**MAC Address**

MAC address of the network element. If you searched on a specific MAC address, this is where that address is displayed.

**Address**

Address (IP, UDP, etc.) of the network element. The next field (Address Type) tells you what type of address this is.

**Address Type**

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

**Host Name**

Host name associated with the network element's IP address, if any.

**User Name**

User ID associated with the network element, if any.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.



---

State	Meaning
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed on this line of the table.

---

**Related Information**

For information on related tasks:

- [Searching MAC Addresses](#)

For information on related windows:

- [Compass Tab](#)

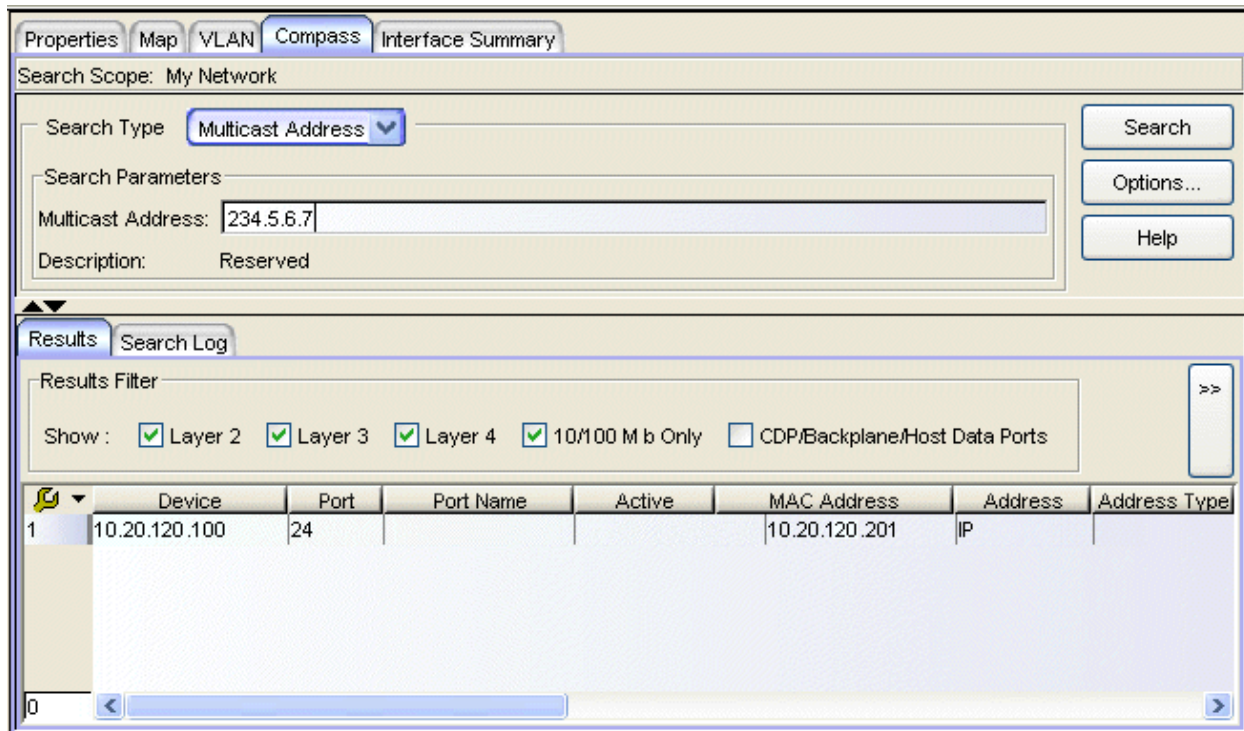
## Compass Tab Multicast Address Search

---

The Multicast Address search on the [Compass tab](#) lets you search any device(s) or device group(s) selected in the left panel for a multicast address. Compass searches the following tables for the specified address.

- ctCDPNeighbor
- ctIfTable
- ctIGMPCacheTable
- ctIGMP MIB
- dot1qVlanCurrentTable
- dot1qVlanStaticTable
- ifTable
- igmpCacheTable
- sysUpTime

To access the Multicast Address search on the Compass tab, select the desired device(s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the Multicast Address Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.



### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the Multicast Address search type from the drop-down list.

### Search Parameters

Compass performs the search within the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To search for information on a specific multicast address, enter it in the Multicast Address text box. If you leave the Multicast Address text field blank, Compass will search for all multicast addresses within the scope. To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

### Multicast Address

Enter the specific multicast address for which you want to search. Compass will look for this address within the selected [scope](#). See <http://www.iana.org/assignments/multicast-addresses> for a list of common multicast address groups.

**Description**

The description of the multicast address you are entering appears here as soon as you type enough of the address for Compass to recognize it.

*Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

*Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu options offered on this tab.

**Device**

This column lists any device which is aware of the multicast address. For example, the network element associated with the multicast address may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

**Port**

Port number of the port which is aware of the multicast address. The network element may be connected to this port.

**Port Name**

Port name of the port which is aware of the multicast address. The network element may be connected to this port.

**Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

**MAC Address**

MAC address of the network element.

**Address**

Address (IP, UDP, etc.) of the network element. The next field (Address Type) tells you what type of address this is.

**Address Type**

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

**Host Name**

Host name associated with the network element's IP address, if any.

**User Name**

User ID associated with the network element, if any.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

MIB or table in which the information displayed on this line of the table was found.

---

**Related Information**

For information on related tasks:

- [Searching Multicast Addresses](#)

For information on related windows:

- [Compass Tab](#)

## Compass Tab

### User Name Search

---

The user name search on the [Compass tab](#) lets you search any device(s) or device group(s) selected in the left panel for a specific user name, a partial user name, or for all user names. The user name search requires that Web-based or 802.1X authentication be supported and enabled on the device(s). Devices which do not support user name searches will be listed in the Compass [Search Log tab](#). The user name search looks at the following tables:

- ctCDPNeighbor
- ctIfTable
- dot1xAuthPaeState
- dot1xAuthSessionStatsTable
- etsysConvEndPointConnMacTable
- etsysDot1xAuthSessionStatsTable
- etsysPwaAuthPwaState

- etsysPwaAuthSessionStatsTable
- ifTable
- sysUpTime

To access the User Name search on the Compass tab, select the desired device (s) or device group(s) in the left panel, and select the Compass tab in the right panel. Then select the User Name Search Type from the drop-down list. If the bottom section of the Compass tab containing the Results and Search Log tabs is not visible, click the panel control up button ▲ at the foot of the tab.

The screenshot shows the Compass tab interface with the following components:

- Search Scope:** My Network->All Devices
- Search Type:** User Name
- Search Parameters:** User Name: qa
- Buttons:** Search, Options..., Help
- Results Filter:** Show:  Layer 2  Layer 3  Layer 4  10/100 Mb Only  CDP/Backplane/Host Data Ports
- Results Table:**

Device	Port	Port Name	Active	MAC Address	Address	Address Type	Host Name	User Name
1	0.20.77.57	1	Fast Ethernet Fro...	00:08:c7:6b:77:da		MAC		qa
2	0.20.77.33	31009	fe.3.9	00:08:c7:6b:77:da		MAC		qa

### Search Scope

The scope within which the search will be performed, based on the device (s) or device group(s) selected in the left panel.

### Search Type

Select the User Name search type from the drop-down list.

### Search Parameters

Compass performs the search on the device(s) or device group(s) selected in the left panel (the [Search Scope](#)). To search for information on a specific user name or a partial user name, enter it in the User Name text field. If you leave the User Name text field blank, Compass will search for all the user names within the

scope. To start a search, click **Search**. You can stop the search at any time by clicking the **Stop** button.

### **User Name**

Enter the specific user name on which you want to search. Compass will look for this name within the selected [scope](#). You can also enter a partial user name; for example, if you entered "tom" as your search criteria, "tommy" and "atom" would be found.

### *Search Log Tab*

This tab displays a log of the progress of the search and notifies you of unsupported devices. See [Search Log Tab](#) for more information.

### *Results Tab*

This tab displays the results of the Compass search in table form. See [Results tab](#) for information on using the Results Filter, and the other right-click menu options offered on this tab.

### **Device**

This column lists any device which is aware of the user name. For example, the network element associated with the user name may be connected to this device, or it may have contacted this device, or this device may be on the path to a device the network element contacted.

### **Port**

Port number of the port which is aware of the network element's user name. The network element may be connected to this port.

### **Port Name**

Port name of the port which is aware of the network element's user name. The network element may be connected to this port.

### **Active**

The checkmarks in this column indicate the entries with the most relevant information. Entries are considered Active if they exist in the 802.1X MIB, PWA MIB, dot1dTpFdb table or the dot1qTpFdb table. To display all the Active entries together, click the Active column header to sort the entries.

### **MAC Address**

MAC address of the network element associated with the user name.



**Address**

Address (IP, UDP, etc.) of the network element. If you searched on a specific user name, this is where that address is displayed. The next field (Address Type) tells you what type of address this is.

**Address Type**

Type of address displayed in the Address field. Possible values include: IP, MAC, UDP.

**Host Name**

Host name associated with the network element's IP address, if applicable.

**User Name**

User ID associated with the network element, if applicable.

**State**

Current operating state of the network element. Possible values are:

<b>State</b>	<b>Meaning</b>
initialize	an initialize is in progress returning the port to an initial state
active	connection is active
inactive,	connection is inactive
disconnected,	no user is logged in.
authenticating	a login is in process and has not yet completed
authenticated	a user has successfully logged in
held	the port is locked down because the number of failed login attempts has exceeded the allowable limit.
connecting	connection in process
aborting	indicates an authentication timeout
forceAuth	the port is always authorized
forceUnauth	an administrator has terminated the user session
authSuccess	means authentication was attempted and succeeded
authTerminated	a session was active or in progress and was subsequently terminated
<blank>.	State was not retrieved

**VLAN Name**

Name of the VLAN associated with the network element, if applicable.

**VLAN ID**

Unique identifier of the VLAN associated with the network element, if applicable.

**Filter ID**

The filtering database used by the VLAN.

**Create Time**

Date and time the network element was first created on the network.

**Multicast Group**

Multicast group address, if applicable.

**Source**

Source (MIB, table) of the information displayed on this line of the table.

---

**Related Information**

For information on related tasks:

- [Searching User Names](#)

For information on related windows:

- [Compass Tab](#)

## Configuration Upload/Download Window

---

The Configuration Upload/Download window provides a way to upload configuration files from devices to save them elsewhere as backups, or download configuration files to devices. Using these functions, you can copy configuration files from one device to another. On some devices, you can also use this window to upload the bootlog file from a device. Files are transferred using TFTP; therefore, you must have a TFTP Server running to perform the upload or download.

To access the Configuration Upload/Download window from the main Console window, right-click the device in the left panel and select **Configuration Upload/Download** from the menu. In Device Manager, select **Utilities > Configuration Upload/Download** from the Device View menu bar.

---

**NOTES:** Console does not support Configuration Upload/Download for the RoamAbout R2.

This window is only available for devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

---

*Sample Configuration Upload/Download window.  
The fields displayed will vary depending on device type and MIB support.*

**Configuration Upload/Download: 10.20.30.40**

**Current Device Settings**

Active Image File:

Active Image Version:

**Operation**

Download Configuration File to Device

Upload Configuration File from Device

Upload Bootlog File from Device

Activate the Last Downloaded Configuration

**Download Settings**

TFTP Server IP:

Server uses Root Path:

Full Image Path:

Path to set on device:

**Status**

Operation Status:

Error Description:

Error Reason:

Bytes Transferred:

Current Values.

## Current Device Settings

The information displayed in Current Device Settings varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

#### Active Image File

Displays the location and filename of the active firmware image.

#### Active Image Version

Displays the firmware image currently active in the device.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

#### Last Server IP

Displays the IP address of the last TFTP server used.

#### Last Filename

Displays the path and filename of the last image downloaded to the device. This is not necessarily the active firmware.

Devices that support *etsysConfigurationManagementMIB* do not provide values for these fields and will display "No Information Provided".

## Operation

The available operations vary depending on the device type. Use the radio buttons to select the desired type of operation:

- **Download Configuration File to Device** -- Performs a download of the specified configuration file to the device. On devices supporting the *ctDL* MIBs, the new configuration file will be activated following the download. Devices supporting the *cfgGroup* MIBs will require the separate [Activate the Last Downloaded Configuration](#) operation in order to activate the new configuration file.
- **Upload Configuration File from Device** -- Performs an upload of the device's active configuration file to the specified file on the TFTP server.
- **Upload Bootlog File from Device** -- Performs an upload of the device's bootlog to the specified file on the TFTP server. This option is only available for devices supporting the *cfgGroup* MIBs.
- **Activate the Last Downloaded Configuration** -- Activates the last downloaded configuration file. This option is only available for devices supporting the *cfgGroup* MIBs.

**NOTE: TFTP Configuration Upload** - When saving a configuration or bootlog file to a new file, Console's TFTP server always creates a new file during the save operation. If you are using a different TFTP server, one that requires that a new file is not automatically created, you should contact Extreme Networks Support at <http://www.extremenetworks.com/support/> for information on how to disable this feature.

## Download Settings

Use this area to specify the download settings.

### TFTP Server IP

Enter the TFTP server's IP address, or use the dropdown list to select the TFTP server to perform the download or upload operation. The list displays IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.

### Server Uses Root Path

If your TFTP server is configured with a root directory, select the checkbox and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to upload or download files to or from this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

### Full Image Path

Enter the full path and filename for the operation. You can also use the drop-down list to select the full path and filename, or use the **Browse** button to navigate to the file. For download operations, specify the name of the configuration file you want to download to the device. For upload operations, specify the name of the file where you want to store the uploaded configuration or bootlog file. (If you are creating a new file, browse to the directory and enter the new filename. The file will be created as part of the transfer operation.) The drop-down list displays the path as set on the device (current), and the last five paths used in this window. If

you have specified a [Root Path](#), the browse capability is limited to the directories below that root path.

### Path to Set on Device

This field displays the target path and filename as it will be set on the device. If the [Server Uses Root Path](#) is selected, the specified root path is stripped from the full path and filename. If [Server uses Root Path](#) is not selected, this field displays the same path as the [Full Image Path](#) field.

## Status

The information displayed in Status varies depending on the device type.

---

**NOTE:** Devices that support *etsysConfigurationManagementMIB* will display dashes (--) in these fields until an operation begins, at which time they will report the progress of that operation.

---

### Operation Status

This field displays the status of the download operation, and varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

- **Idle** -- the device is currently not engaged in a transfer, and no error has occurred.
- **Sending** -- the device is uploading a configuration file or bootlog file to the server.
- **Receiving** -- the device is having a configuration file downloaded to it.
- **Transfer Complete** -- the transfer operation completed successfully.
- **Error** -- an error occurred during the transfer. Refer to the [Error Description](#) and [Error Reason](#) fields for more information.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

- **Normal Operation** -- following a transfer, indicates that the operation was completed successfully. Also indicates the device is operating within normal parameters.

- **Download Active** -- the device is currently processing a TFTP download.
- **Error Detected During Download** -- a download was started but an error was detected. See the [Error Description field](#) for more information.
- **Other/Unknown** -- the device is in an unspecified or unknown state.

For devices that support *etsysConfigurationManagementMIB*, the information is displayed as follows:

- **Inactive** -- the device is currently not engaged in a transfer.
- **Pending** -- the transfer operation is in queue.
- **Running** -- the transfer operation is in progress.
- **Success** -- the transfer operation completed successfully.
- **Error Detected During Operation** -- an error occurred during the transfer. See the [Error Description field](#) for more information.

#### Error Description

Displays a description of any error detected during a download. For devices that support the *cfgGroup* MIBs, it could be any of the following descriptions:

- **No Error** -- no errors were reported.
- **Timeout** -- a timeout error occurred.
- **Network Error** -- an error occurred on the network.
- **Device Memory Error** -- usually indicates the device's memory space is full.
- **Invalid Configuration** -- the downloaded configuration file was not valid for the device type.
- **Command Completed** -- the command issued to the device was completed successfully.
- **Internal Error** -- an error occurred on the device.
- **TFTP Server Error** -- an error occurred between the device and the server.

#### Error Reason

Displays a reason for any error detected during a download. This field is only displayed for devices that support the *cfgGroup* MIBs.



### Bytes Transferred

Depending on the device and the TFTP server being used, this field may display transfer statistics during an operation. In some cases, a progress bar will also appear at the bottom of the screen (in the status bar), reporting the percentage of the transfer completed.

### Apply Button

Sets the configured information to the device and starts the specified operation.

### Refresh Button

Resets the fields to default values, as reported by the device.

---

## Related Information

For information on related tasks:

- [How to Save and Restore Configuration Files](#)

For information on related windows:

- [Firmware Image Download Window](#)

# Extreme Management Center Console Options (Legacy)

---

These options apply only to the Extreme Management Center's Console application. In the Options window (**Tools > Options**), the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Console folder to view all the different options you can set.

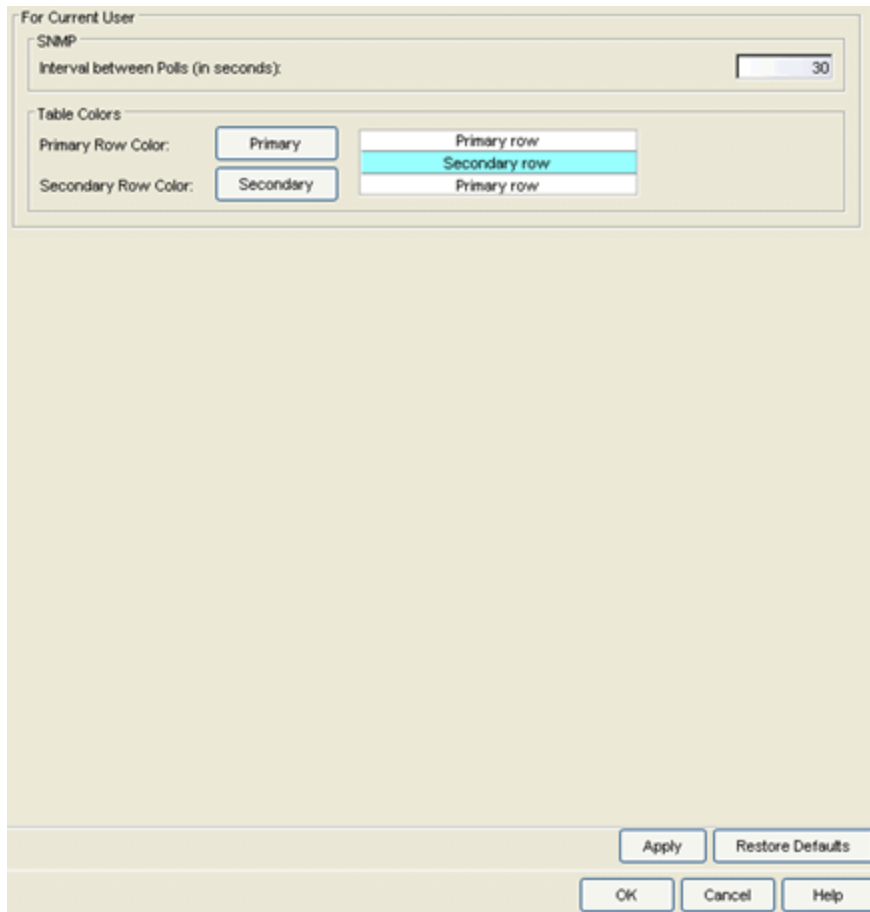
Information on the following Console options:

- [Device Manager](#)
- [Discover](#)
- [FlexView](#)
- [Welcome View](#)
- [Property View](#)
- [Compass](#)
- [VLAN View](#)
- [Basic Policy View](#)
- [Wireless Manager](#)
- [Policy Control Console](#)
- [RoamAbout Wireless Manager](#)
- [TopN Collector](#)
- [NetFlow Collection](#)
- [OneView](#)
- [OneView Dialog Boxes](#)
- [OneView Collector](#)
- [OneView Engine](#)
- [ACL Manager](#)

## Device Manager

Selecting Device Manager in the left panel of the Options window provides the following view where you can specify Device Manager polling options and the

colors you want to use in Device Manager tables. Device Manager uses the polling cycles specified here to contact the device and update Device View information.



### Interval between poll cycles

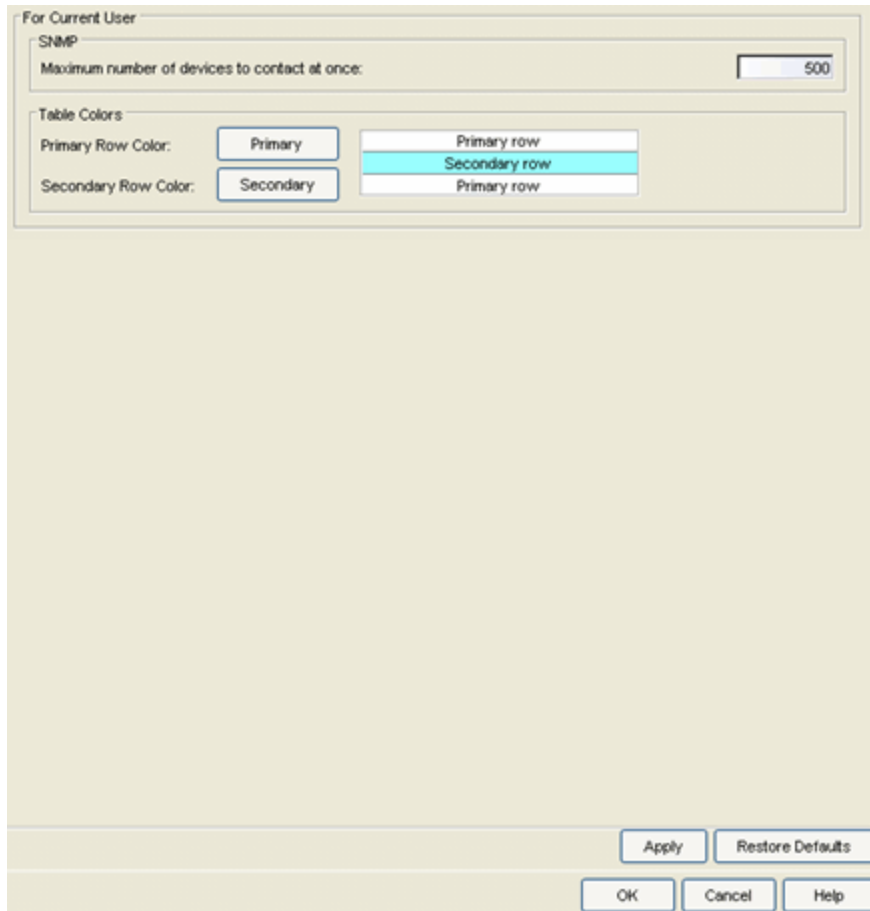
The amount of time (in seconds) that Device Manager waits between polling the device.

### Device Manager 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.

## Discover

Selecting Discover in the left panel of the Options window provides the following view where you can specify options for the Console Discover operation.



### Maximum number of devices to contact at once

The number of IP addresses Discover will try to contact simultaneously. Discover works with blocks of IP addresses, starting a new block each time the outstanding block completes.

### Discover Table Colors

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.

## FlexView

Selecting FlexView in the left panel of the Options window provides the following view where you can specify polling options for the web-based and Console FlexView tables and graphs, the colors used in FlexView tables, and the default export directory for FlexViews.

### *For All Users*

These settings specify the polling options for web-based FlexViews accessed through the Management Center's **Network** tab. These settings applies to all users.

#### **Maximum number of devices to contact at once**

The number of devices that will be contacted simultaneously. The Management Center server polls blocks of IP addresses, starting a new block each time the outstanding block completes.

### *For Current User*

These settings specify options for FlexViews accessed through Console. These settings will apply to the current logged-in user.

#### **Maximum number of devices to contact at once**

The number of devices that Console will try to contact simultaneously. Console polls blocks of IP addresses, starting a new block each time the

outstanding block completes.

### FlexView 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.

### Export Directory

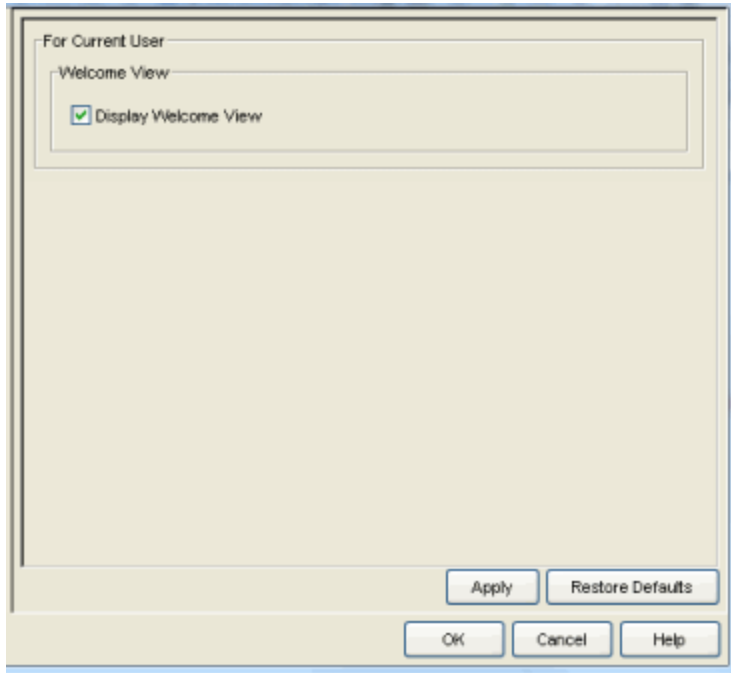
In FlexView Properties, you can configure FlexView table information to be automatically exported with each table refresh, using the Export Type parameter. The exported information is saved by default to the directory specified here.

### Advanced Editor

The **Use OID Name** option specifies that the OID name will be used instead of the numeric OID in the XML encoding for the FlexView. Deselecting this option lets you create FlexViews with OID-based SNMP columns that are unique.

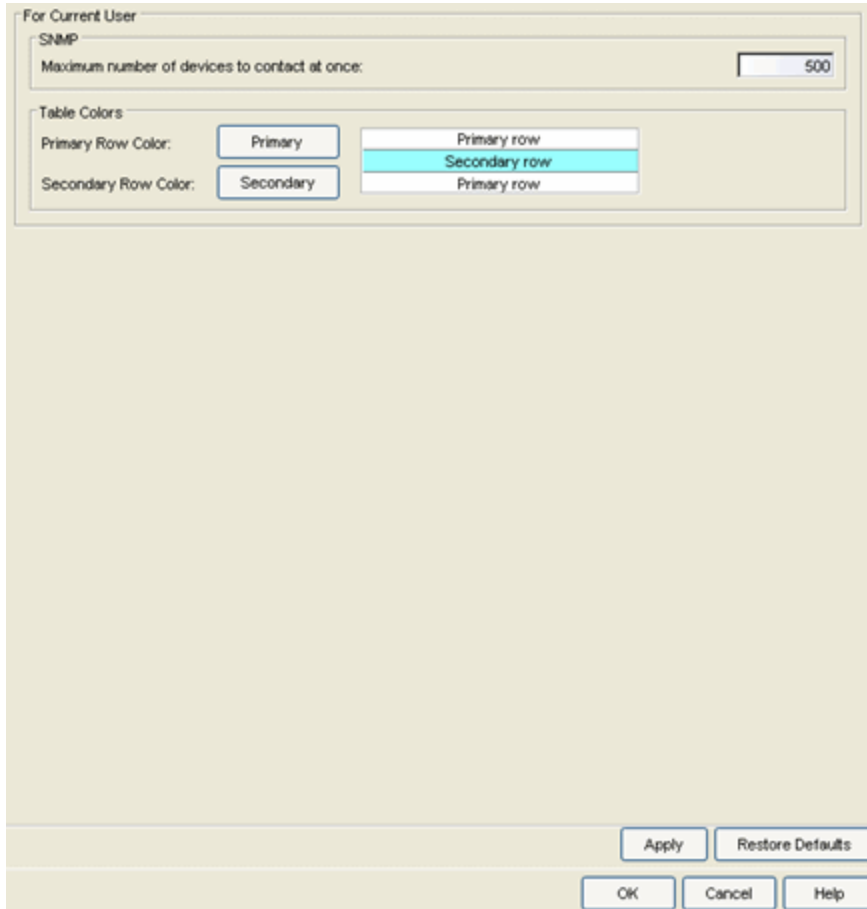
## Welcome View

Selecting Welcome View in the left panel of the Options window provides the following view where you can enable or disable the display of the right-panel **Welcome** tab. The **Welcome** tab is available when the top-level My Network folder is selected in the left-panel tree. It provides links to Console tasks such as Management Center Discover and Authorization/Device Access windows, and also provides access to video tutorials on these tasks.



## Property View

Selecting Property View in the left panel of the Options window provides the following view where you can specify options that define the SNMP polling parameters and appearance of the **Properties** tab in Console.



### Maximum number of devices to contact at once

The number of devices Console will try to contact simultaneously. Console works with blocks of IP addresses, starting a new block each time the outstanding block completes.

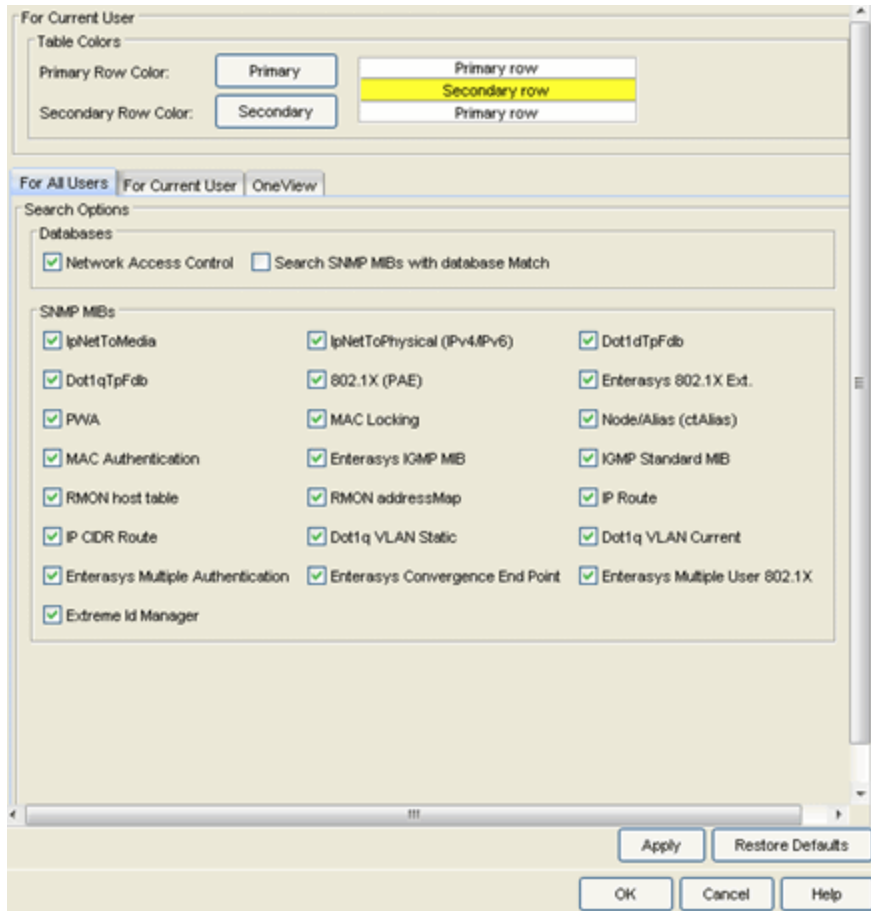
### Properties Tab Table Colors

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.

## Compass

Selecting Compass in the left panel of the Options window provides the following view where you can specify Compass SNMP and Search options.





### Compass 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.

### Search Options

The boxes that are checked in this section determine which data sources will be used with Compass searches. By default, Compass is configured to include the NAC Manager database (the "Network Access Control" checkbox) as well as various SNMP MIB objects when performing searches. (Refer to the [MIB/Table Descriptions](#) topic for information about MIB selections.) The Compass search begins by resolving IP address to MAC address in order to start searching for MAC-IP pairs from the network. When a match is found in the NAC Database, the SNMP MIBs will **not** be searched unless the "Search SNMP MIBs with database Match" checkbox is also selected. If the "Network Access Control" checkbox is deselected, then the NAC Manager Database will not be used to resolve IP address to MAC address. You can specify search options in three different tabs:

- **For All Users** - These search options apply for all users on all Management Center clients.
- **For Current User** - These options let you override the All Users search options and instead use this set of search options for the current user. These settings are stored in the user's home directory and apply only to the Management Center client running on this machine or machines with shared access to the user's home directory.
- **OneView** - These options are for the Compass search in Management Center. In addition to search options, they include search limit settings which are used to help limit the Management Center server resources used for the searches:
  - **Number of searches allowed at once.** The maximum number of Compass searches that can be performed at one time.
  - **Number of search results allowed.** The maximum number of search results that can be displayed in the table.
  - **Number of devices allowed for a search.** The maximum number of devices that can be included in a search.
  - **Time limit for a search.** The maximum search time in seconds.

### VLAN View

Selecting VLAN View in the left panel of the Options window provides the following view where you can specify options that define the SNMP polling parameters and appearance of the **VLAN** tab in Console.

For Current User

SNMP

Maximum number of devices to contact at once:

Table Colors

Primary Row Color: 

Primary row
Secondary row
Primary row

Secondary Row Color:

Enable Display of Port Elements

Port Elements in VLAN Advanced/Basic Port

Default VLAN Port Sort

By IP / Port  By IP / Name  By Last User Sort

Apply Restore Defaults

OK Cancel Help

### Maximum number of devices to contact at once

The number of IP addresses Console will try to contact simultaneously. Console works with blocks of IP addresses, starting a new block each time the outstanding block completes.

### VLAN 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 Elements

Selecting this checkbox filters the port views based on selected port elements, making it easier to use VLAN Manager with groups of port elements.

### Default VLAN Port Sort

Use the radio buttons to specify how the data in the **VLAN Basic Port** tab will be sorted by default when the device data is retrieved: by IP address and Port, by IP address and Name, or by the sort used by the last user. The

"By Last User Sort" option allows you to continue to use the last sort options you had configured using the Sort Toolbar (available from the right-click menu on a table entry). For example, if you had the sort set to Port (descending) and PVID (ascending) and you close the application, then the next time you open the application, the tab will use that same sort.

## Basic Policy View

Selecting Basic Policy View in the left panel of the Options window provides the following view where you can specify options that define the SNMP polling parameters and appearance of the **Basic Policy** tab in Console.

The screenshot shows a dialog box titled "For Current User" with the following sections:

- SNMP**: A section containing a label "Maximum number of devices to contact at once:" and a text input field with the value "500".
- Table Colors**: A section with two rows of color selection:
  - Primary Row Color:** A button labeled "Primary" and a color selection box showing "Primary row" (white) and "Secondary row" (light blue).
  - Secondary Row Color:** A button labeled "Secondary" and a color selection box showing "Primary row" (white) and "Secondary row" (light blue).

At the bottom of the dialog, there are four buttons: "Apply", "Restore Defaults", "OK", "Cancel", and "Help".

### Maximum number of devices to contact at once

The number of devices that Console will try to contact simultaneously. Console polls blocks of IP addresses, starting a new block each time the outstanding block completes.

## Basic Policy Tab Table Colors

Use the buttons to select the primary and secondary row colors you want to use in tables in the **Basic Policy** tab. A sample of your selection will be displayed in the sample table scheme to the right of your selections.

## Wireless Manager

Selecting Wireless Manager in the left panel of the Options window provides the following view where you can specify options for the Wireless Manager application.

The screenshot shows a configuration window for the Wireless Manager application. It is divided into two main sections: "For All Users" and "For All Sessions On This Machine".

**For All Users:**

- Shared Secret:** A text field labeled "Default Shared Secret:" contains the value "10dmcj#ru57hvid".
- History:** A text field labeled "Maximum Number of Executed Tasks to retain in Task History:" contains the value "100".
- Audit:**
  - A time picker labeled "Audit Start Time [time of day]:" is set to "03:00".
  - A text field labeled "Audit Interval [run audit every]:" contains the value "24 hours".

**For All Sessions On This Machine:**

- Table Colors:**
  - Primary Row Color:** A button labeled "Primary" is selected. To its right is a preview table with three rows: "Primary row" (white), "Secondary row" (light blue), and "Primary row" (white).
  - Secondary Row Color:** A button labeled "Secondary" is selected. To its right is a preview table with three rows: "Primary row" (white), "Secondary row" (light blue), and "Primary row" (white).

At the bottom of the window are four buttons: "Apply", "Restore Defaults", "OK", "Cancel", and "Help".

## Shared Secret

Any time Management Center discovers a new controller, Wireless Manager will attempt to authenticate with the controller using this shared secret. For proper functioning of Management Center, Wireless Manager, and Wireless Advanced Services, the controller must be configured with the same shared secret as Wireless Manager. Each controller can be configured with a different shared secret as long as Wireless Manager knows what it is. You can configure Shared Secrets on a per controller basis using Wireless Manager. Please refer to the Wireless Manager online Help for additional details.

## History

After a task has executed, it is retained in the Wireless Manager database to provide a detailed history of task activity. A large amount of information is kept for each executed task, including the complete CLI script executed against each target controller. To maintain the database at a reasonable size, Wireless Manager keeps only a fixed number of executed tasks in the database. When the task limit is reached or exceeded, Wireless Manager deletes the oldest executed tasks from its database. The History option allows you to control how many task definitions Wireless Manager will retain in its database. The default is 100 executed tasks retained, and the maximum is 500 tasks retained.

## Audit

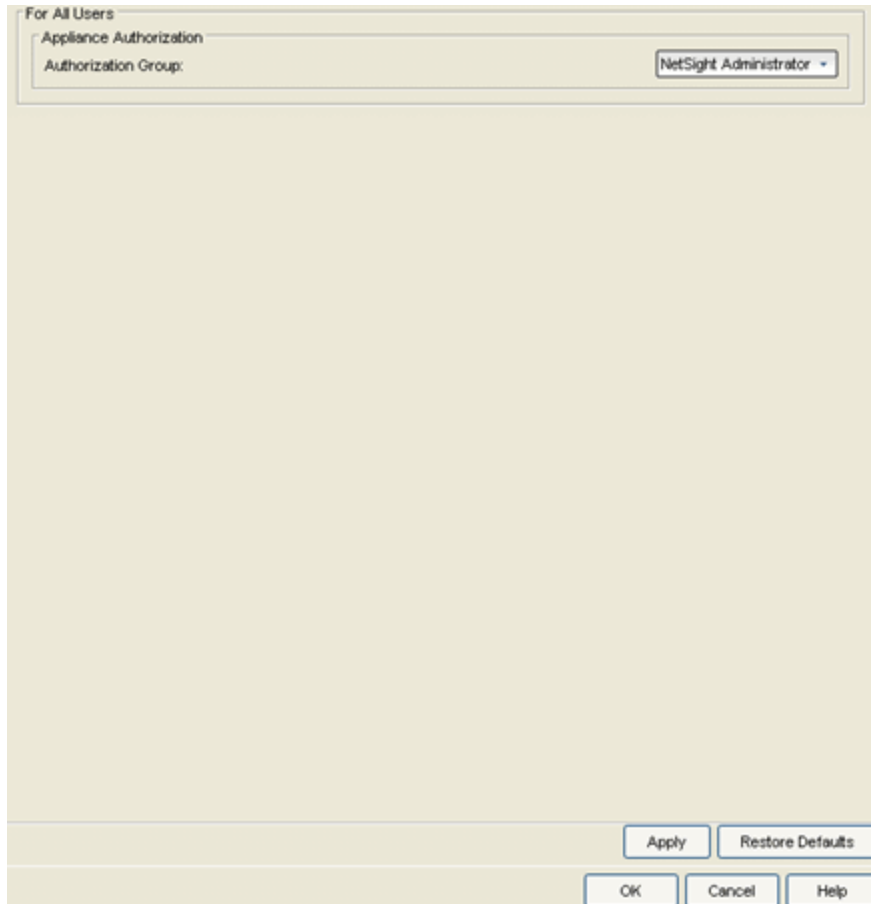
Wireless Manager audits controller configuration to ensure that it does not deviate from the deployed templates. When Wireless Manager encounters discrepancies between the template and the actual controller configuration, the audit feature logs an error. You can manually run an audit or you can schedule automatic audits using these Audit options. Select the time of day when the audit should start and the interval in hours between the start of successive audits. Auditing once every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

## Table Colors

You can customize the appearance of the screens in Wireless Manager by applying contrasting colors to alternating table rows. From the drop-down menu, select row colors for alternating primary and secondary rows. A sample to the right provides a snapshot of the way table colors will display on the screen.

## Policy Control Console

Selecting Policy Control Console (PCC) in the left panel of the Options window provides the following view where you can specify options that define the SNMP polling parameters for the PCC tool and the authorization group for the PCC appliance.

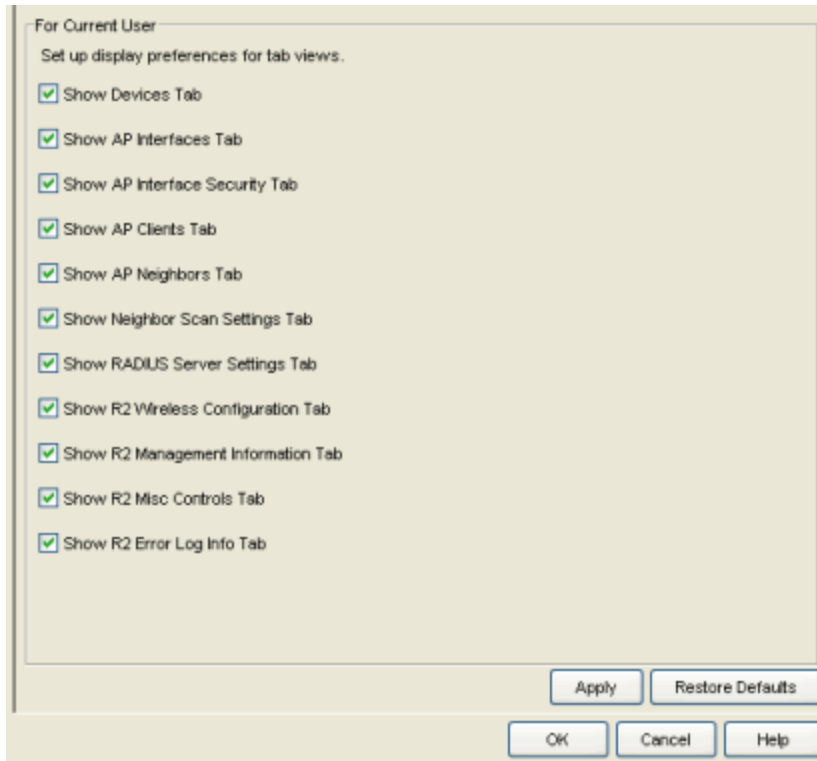


### Appliance Authorization Group

Use the drop-down list to select the Authorization Group with the correct profile for the PCC appliance to use when communicating with devices. Profiles define the level of device access granted to users that are members of that Authorization Group. Profiles and Authorization Groups are defined in the Authorization/Device Access window (Tools > Authorization/Device Access).

### RoamAbout Wireless Manager

Selecting RoamAbout Wireless Manager in the left panel of the Options window provides the following view where you can specify which right-panel tabs you want displayed in the RoamAbout Wireless Manager main window.

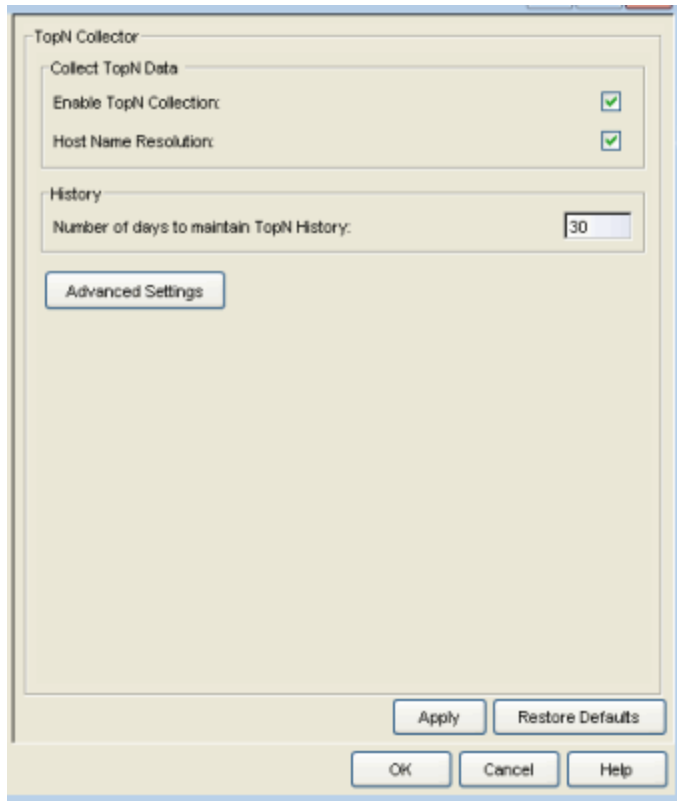


## TopN Collector

The TopN Collector collects the data used in Management Center TopN reports. It also collects the signal strength data reported by Wireless Controllers.

You can use this view to enable or disable TopN collection and host name resolution, and specify the number of days to maintain the TopN History. See below for more information on these options.





### Enable TopN Collection

This option allows you to enable and disable the TopN Collector. Changes to this option take place immediately.

### Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for TopN only. (Host name resolution is enabled globally using the Suite Name Resolution option.) Changes to this option take place immediately.

### Number of days to maintain TopN History


This setting determines how many days of TopN information will be available for viewing in the reports. The default number of days is 30, with a minimum value of 1 day and a maximum value of 180 days. Changes to this option take effect with the next nightly TopN history cleanup task performed by the Management Center server.

### Advanced Settings

Click the **Advanced Settings** button to open the [TopN Collector Advanced Settings window](#) where you can configure more advanced collector options.

## NetFlow Collection

Selecting NetFlow in the left panel of the Options window provides the following view where you can configure NetFlow flow collection settings.



The screenshot shows the 'NetFlow Collection' configuration window. It features a 'NetFlow Settings' section with the following options:

- Enable NetFlow Collector:
- Maximum Flows To Maintain In Memory:
- Maximum Aggregate Flows To Maintain In Memory:
- Maximum Number Of Flows Allowed Per Table View:
- Send/Receive NetFlow Data On Socket:
- Export Interval (minutes):
- NetFlow v9 Template Refresh Rate (packets):
- NetFlow v9 Template Timeout (minutes):
- NetFlow Host Name Resolution:
- NetFlow Port Name Resolution:

Below the settings is an 'Advanced Settings' button. At the bottom of the window are 'Apply', 'Restore Defaults', 'OK', 'Cancel', and 'Help' buttons.

### Enable NetFlow Collector

Use this checkbox to enable/disable NetFlow packet processing on the Management Center server, allowing you to turn off NetFlow for troubleshooting purposes. When NetFlow is enabled or disabled, a message is logged to the Console log as well as the Management Center server log. When NetFlow is disabled, the Application Flows report on the Management Center **Flows** tab is cleared. However, the Flow Engine Summary on the Management Center **Administration** tab continues to show the statistics for previous flows.

### Maximum Flows to Maintain in Memory

Changing this number would adjust the amount of memory used to store flows.

### **Maximum Aggregate Flows to Maintain in Memory**

Changing this number would adjust the amount of memory used to store aggregated flows.

### **Maximum Number of Flows Allowed Per Table View**

Sets the maximum number of flows that can be displayed in Management Center NetFlow reports.

### **Send/Receive NetFlow Data on Socket**

The port on the Management Center server that listens for flow collection data. If you change this port number here, you also need to reconfigure the port number on the switch.

### **Export Interval**

This is the active timer which determines the maximum amount of time a long-lasting flow will remain active before expiring. When a long-lasting active flow expires due to the active timer expiring, another flow is immediately created to continue the ongoing flow. The Management Center flow collector rejoins these multiple flow records to report a single logical flow.

### **NetFlow v9 Template Refresh Rate**

The number of export packets sent before the flow sensor retransmits a template to the collector when using NetFlow Version 9.

### **NetFlow v9 Template Timeout**

The number of minutes the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.

### **NetFlow Host Name Resolution**

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option enables host name resolution for NetFlow only. Host name resolution for the Management Center Suite is enabled globally using the Management Center Suite-Wide Name Resolution option. The Suite-Wide option must be enabled for this NetFlow option to take effect.

### **NetFlow Port Name Resolution**

Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to disable port name resolution for NetFlow only. (Port name resolution is enabled globally using the Suite Name Resolution option.)

## Advanced Settings

Click the Advanced Settings button to open the [NetFlow Advanced Settings window](#) where you can configure advanced options.

## OneView

The OneView options let you specify SNMP polling options for the real-time data collection used in the Management Center Search (PortView) **Overview** tab.

You can also adjust the maximum number of **FlexView** or **PortView** tabs that can be displayed in Management Center at one time. For example, the default limit of five PortViews allows you to have five active searches open at one time. Changing the limit to ten would allow you to have ten active searches open at one time. Keep in mind that adjusting these settings to a higher number could impact Management Center performance.

You can also use this view to set the Date and Time format to be used in Management Center reports.

The screenshot shows the 'OneView' configuration window with the following sections and settings:

- Session Limits:**
  - The maximum number of FlexViews that can be displayed:
  - The maximum number of PortViews that can be displayed:
- Date/Time Format:**
  - Date:**
    - MMDD/YYYY
    - YYYY/MMDD
    - DD/MM/YYYY
    - Month DD, YYYY
  - Time:**
    - 12 Hour Format
    - 24 Hour Format
- Display MAC Addresses by:**
  - Full MAC Address (00:01:F4:22:22:22)
  - MAC OUI Prefix (Enterasys Networks: 22:22:22)
  - Limit OUI to first  characters
  - Display Unknown MACs as Unknown
- Map Settings:**
  - Status Refresh Interval:
- How to display devices in the device tree:**
  - Use IP Address
  - Use System Name
  - Use User Defined Nickname

Buttons at the bottom: Apply, Restore Defaults, OK, Cancel, Help.

### Session Limits

Use these settings to specify the maximum number of **FlexView** and **PortView** tabs per Management Center server that can be displayed in Management Center at one time. Adjusting these settings to a higher number could impact Management Center performance.

### 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.

### Display MAC Addresses by

Specify how you want to display end-system MAC addresses in the Management Center Wireless client and threat tables, as well as the Access Control end-system 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".

### Status Refresh Interval

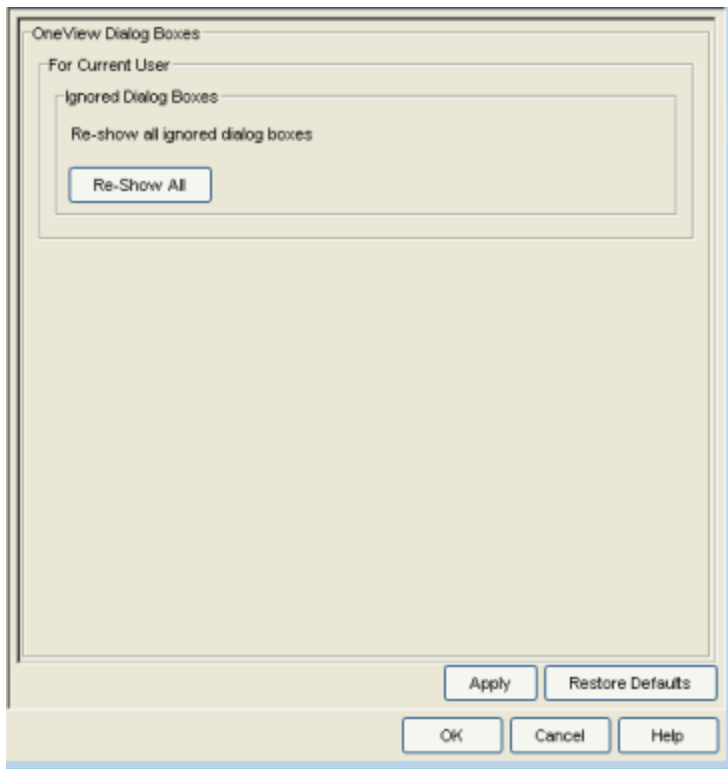
Management Center maps display an integrated alarm/device status either to the right of a device or AP image, or incorporated as part of a map marker. The alarm status automatically refreshes every 30 seconds by default. Use the drop-down list to change the refresh interval, if desired. This option provides a way to adjust the load on the Management Center server if status requests are causing performance issues. You can change the setting to a longer interval or to None, as your situation requires.

### How to display devices in the device tree

This setting determines how devices are displayed in the My Network navigation tree. You can set the device tree to display devices by IP address, system name, or user-defined nickname by selecting **Use IP Address**, **Use System Name**, **Use User Defined Nickname**, respectively.

## OneView Dialog Boxes

The OneView Dialog Boxes option lets you re-show all message dialog boxes that you have turned off in Management Center (for example, if you have selected the "Do not show this message again" checkbox on a Warning dialog). This setting applies only to the current user.



## OneView Collector

The OneView Collector options let you specify SNMP polling options for Management Center (formerly OneView) data collection, enable and disable statistics collection, and access advanced settings for the OneView Collector. The OneView Collector gathers historical reporting data over time, which is then used in Management Center reports.

The screenshot shows the 'OneView Collector' configuration window. It is divided into four main sections, each with a title bar and a list of settings:

- Wireless Collection:**
  - Collect Statistics:
  - Access Point Poll Rate (minutes):
  - Controller Poll Rate (minutes):
  - Edit Include/Exclude Filter List:
  - Edit Client History and Threat options:
- Device Collection:**
  - Collect Statistics:
  - Collect Additional Extreme/Enterasys Statistics:
  - Collect Host Resource Statistics:
  - Poll Rate (minutes):
- Interface Collection:**
  - Collect Statistics:
  - Collect Additional Extreme/Enterasys Statistics:
  - Poll Rate (minutes):
- NAC Collection:**
  - Collect NAC Statistics:
  - Poll Rate (minutes):

At the bottom of the window, there is an 'Advanced Settings' button. Below the main configuration area are 'Apply' and 'Restore Defaults' buttons. At the very bottom are 'OK', 'Cancel', and 'Help' buttons.

## Wireless Collection

### Collect Statistics

Use this checkbox to enable or disable wireless data collection.

### Access Point Poll Rate

The amount of time (in minutes) that the data collector waits between polling wireless access points. Valid values are 1-60 minutes.

### Controller Poll Rate

The amount of time (in minutes) that the data collector waits between polling wireless controllers. Valid values are 1-60 minutes.

### Edit Include/Exclude Filter List

Use this option to filter the client events displayed in the Management Center Wireless Client History, Top Clients by Bandwidth, and Client Event History reports. Click the **Edit** button to open a window where you can use the drop-down menu to select whether to display client events for:

**All SSIDs and Topologies** - Client events for all SSIDs and Topologies will

be displayed.

**Some SSIDs** - Select the SSIDs to include or exclude.

**Some Topologies** - Select the Topologies to include or exclude. The Client Event History report does not support the ability to filter on topologies.

### **Edit Client History and Threat options**

Click the **Edit** button to open a window where you can configure Wireless History Settings. These settings pertain to the Management Center Wireless Client Event History report.

### *Device Collection*

#### **Collect Statistics**

Use this checkbox to enable or disable device data collection.

#### **Collect Additional Extreme/Enterasys Statistics**

Use this checkbox to enable or disable Extreme or Enterasys switch resource statistics collection.

#### **Collect Host Resource Statistics**

Use this checkbox to enable or disable host resource statistics collection.

#### **Poll Rate**

The amount of time (in minutes) that the data collector waits between polling devices. Valid values are 1-60 minutes.

### *Interface Collection*

#### **Collect Statistics**

Use this checkbox to enable or disable interface data collection.

#### **Collect Additional Extreme/Enterasys Statistics**

Use this checkbox to enable or disable Extreme or Enterasys interface statistics collection.

#### **Poll Rate**

The amount of time (in minutes) that the data collector waits between polling interfaces. Valid values are 1-60 minutes.

### *NAC Collection*

#### **Collect Statistics**

Use this checkbox to enable or disable NAC data collection.



## Poll Rate

The amount of time (in minutes) that the data collector waits between polling Access Control engines. Valid values are 1-60 minutes.

## Advanced Settings

Click the Advanced Settings button to open the [OneView Collector Advanced Settings window](#) where you can configure advanced options.

## OneView Engine

Selecting OneView Engine in the left panel of the Options window provides the following view where you can specify data aging options and advanced settings for data archiving and aggregation.

The screenshot shows the 'OneView Engine' configuration window. It is divided into two main sections: 'Data Aging' and 'Server CPU Reporting'. The 'Data Aging' section contains five input fields for different data types: 'Length of time to maintain collection data (days)' with a value of 7, 'Length of time to maintain hourly archive data (weeks)' with a value of 8, 'Length of time to maintain daily archive data (months)' with a value of 6, 'Length of time to maintain weekly archive data (months)' with a value of 12, and 'Length of time to maintain monthly archive data (months)' with a value of 12. The 'Server CPU Reporting' section has one input field for 'The interval for reporting average and maximum CPU (minutes)' with a value of 5. Below these sections is a button labeled 'Advanced Settings'. At the bottom of the window are three buttons: 'Apply', 'Restore Defaults', and 'OK', 'Cancel', and 'Help'.

## Data Aging

Data aging options determine how long the collection data used by Management Center reports is maintained in the Management Center database. You can set an aging value for each of the following data types:

- collection data - This setting specifies how long (in days) to maintain the raw data collected by the data collector. Valid values are 1-1000 days.
- hourly data - Every hour, the raw data is condensed into hourly average values and archived. This setting specifies how long (in weeks) to maintain the archived hourly data. Valid values are 1-800 weeks.
- daily data - Every day, the hourly data is condensed into daily average values and archived. This setting specifies how long (in months) to maintain the archived daily data. Valid values are 1-200 months.
- weekly data - Every week, the daily data is condensed into weekly average values and archived. This setting specifies how long (in months) to maintain the archived weekly data. Valid values are 1-200 months.
- monthly data - Every month, the weekly data is condensed into monthly average values and archived. This setting specifies how long (in months) to maintain the archived monthly data. Valid values are 1-200 months.

### Server CPU Reporting

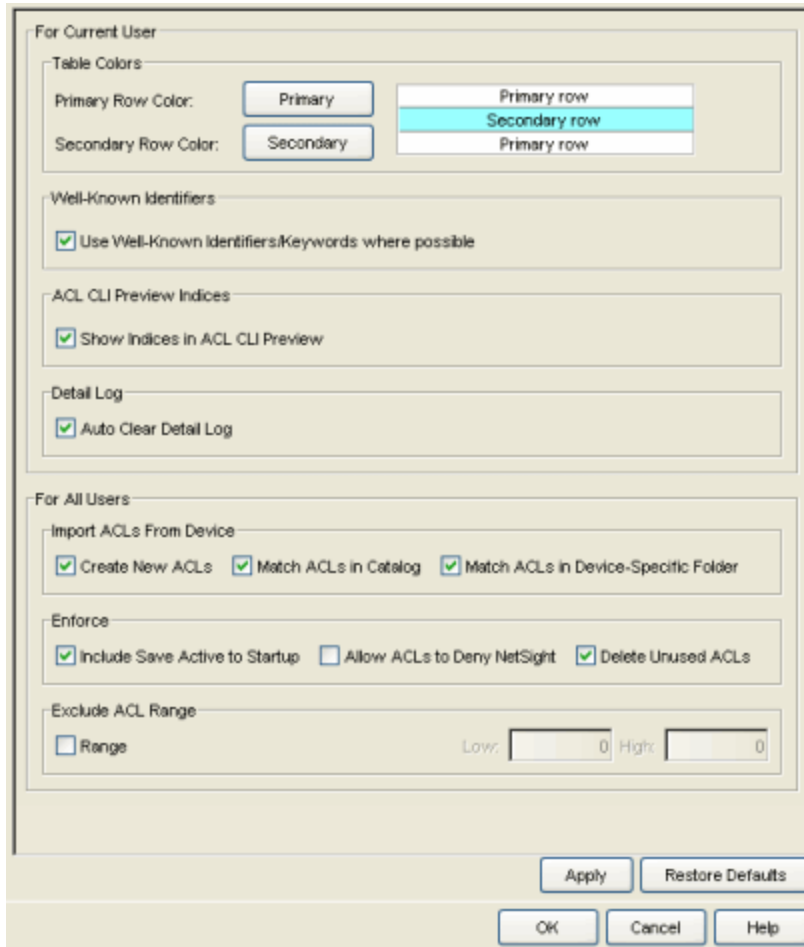
Extreme Management Center collects Management Center server CPU usage statistics to monitor the Management Center server usage. At 5 minute intervals (the default interval) the collected usage data is averaged, and the average and maximum statistics are reported to the Management Center database to provide data for the Management Center Server CPU Utilization report. You can change the default interval setting here, if desired. A shorter interval would provide a more granular picture of CPU usage while a longer interval would mean that less data is stored in the database. Valid values are 1-59 minutes.

### Advanced Settings

Click the Advanced Settings button to open the [Engine Advanced Settings window](#) where you can configure advanced data archiving, data aggregation, and session limit options.

## ACL Manager

Selecting ACL Manager in the left panel of the Options window provides the following view where you can specify options for ACL Manager.



### ACL Manager 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.

### Well-Known Identifiers

This option lets you select whether to show the well-known identifier protocol when displaying ACL rules in the **ACL Editor** tab.

### ACL CLI Preview Indices

Select the checkbox to display line numbers in the **ACL Editor CLI Preview** tab.

### Detail Log

Select the checkbox if you would like to have the ACL Manager Detail Log automatically cleared when Management Center Console is restarted.

## Import ACLs from Device

Use the checkboxes to select the following parameters when performing an ACL import from a device:

- **Create New ACLs** - ACL Manager compares the imported ACLs against ACLs already within the Catalog folder and device-specific folders, checking for duplicates. If a duplicate ACL is found, the ACL is not imported and ACL Manager uses the existing ACL. If a duplicate ACL is **not** found and this option is selected, a new ACL is created in the ACL Manager database. If this option is not selected, a new ACL will not be created.
- **Match ACLs in Catalog** - Use this option to specify whether or not ACL Manager will compare imported ACLs against ACLs already within the Catalog folder.
- **Match ACLs in Device-Specific Folder** - Use this option to specify whether or not ACL Manager will compare imported ACLs against ACLs already within the device-specific folders.

## Enforce

Use the checkboxes to select the following Enforce operation parameters:

- **Include Save Active to Startup** - When this option is selected, the Enforce operation saves the Active Configuration to the Startup Configuration for the selected device. The default setting is checked.
- **Allow ACLs to Deny (Management Center) NetSight** - When this option is selected, ACL Manager no longer checks for ACLs which deny access to the device from the Management Center server. Use of this option could result in lost contact with the device. If contact is denied by an ACL, you must use the device's command line interface (CLI) to remove the ACL and restore contact. The default setting is unchecked.
- **Delete Unused ACLs** - When this option is checked, ACL Manager will delete any unused ACLs on devices where it performs an Enforce. ACL Manager considers ACLs that are currently defined on a device, but not currently applied to any interfaces or in use by other facilities on the device as Unused. The default setting is checked.

## Exclude ACL Range

This option lets you define a range of ACLs that cannot be used by ACL Manager when allocating a new name for an ACL on a device. For example,

let's say the excluded range is 101-103:

- If you create a new ACL named "new\_acl" and assign it to an interface on a device, when you enforce, ACL Manager determines that ACL "new\_acl" needs to be copied to the device. It also determines that "new\_acl" is an invalid name on that device because the device only supports numbered ACLs. Therefore, ACL Manager must assign a new name for the ACL on the device. The ACL is an extended ACL, and only ACLs 100-199 can be considered for extended ACLs. So, ACL Manager considers using 100. If 100 is already in use, ACL Manager will consider 101. But 101 is excluded. So ACL Manager will consider 102, 103, and finally 104. 104 is not used and not excluded, so it will be used as the new ACL name on the device.
- If you create a new ACL named 102, and assign it to an interface on a device, when you enforce, ACL Manager determines that ACL 102 needs to be copied to the device. It also determines that 102 is an invalid name on that device because it is in the excluded range. Therefore, ACL Manager must assign a new name for the ACL on the device. The ACL is an extended ACL, and only ACLs 100-199 can be considered for extended ACLs. So ACL Manager will consider using 100. If 100 is already in use, ACL Manager will consider 101. But 101 is excluded. So ACL Manager will consider 102, 103, 104, and finally 105. 105 is not used and not excluded, so it will be used as the new ACL name on the device.

#### **Apply Button**

Sets the currently defined settings and keeps the Options window open.

#### **Restore Defaults Button**

Sets the Options settings in the currently selected view to the (default) values that existed when Console was first installed. Fields are cleared for options that do not have default settings.

#### **OK Button**

Sets the options and closes the window.

#### **Cancel Button**

Cancels any changes you have made and closes the window.

---

### **Related Information**

For information on related tasks:

- [How to Set Console Options](#)

## Discover Window


---

The Discover window allows you to discover the physical elements (devices) of your network, and add them to the NetSight database. You can perform a discover on a specified range of IP addresses, or perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices. Discover automatically explores the defined network segment and creates a list of discovered devices. You can then save the discovered devices to the Console database where they are displayed in the left-panel tree.

At the top of the window there are two tabs: IP Range and CDP Seed IP. Select the appropriate tab based on what type of discover you want to perform:

- [IP Range](#) -- perform a discover based on one or more IP address ranges. An IP Range Discover discovers all devices within the specified IP address range(s).
- [CDP Seed IP](#) -- performs discover operations of CDP-compliant devices in the network, starting with a one or more CDP seed devices.

Deciding what type of discover to use depends on your specific network configuration. Generally, if your network has all CDP-compliant devices that are configured with the same SNMP access parameters, the CDP Seed IP Discover is recommended. If your network has no CDP-compliant devices, or a mix of CDP and non-CDP-compliant devices, the IP Range Discover is recommended.

Access the Discover window by selecting **Tools > Discover** in the menu bar or by clicking the Discover button  in the toolbar.

## Configuring Ping for Linux and Mac OS X Clients

The first time you run a **Ping Only Discover** from a Mac OS X or Linux client, the Discover will fail because jping is not executable. To fix this problem, perform the following steps to give the jping executable root privileges, allowing it to open up a socket for communication back to a NetSight client.

**On a Linux client (32-bit or 64-bit):**

1. Open an xterm where you are logged in as root.
2. `mkdir -p /var/Extreme_Networks/NetSight`

3. `cp ~/NetSight/System/<.bin32 or .bin64>/jping /var/Extreme_Networks/NetSight`
4. `chmod a+x /var/Extreme_Networks/NetSight/jping`
5. `chmod u+s /var/Extreme_Networks/NetSight/jping`

#### On a Mac OS X client (64-bit):

1. Open a terminal window.
2. `cd ~/NetSight/System/.bin64`
3. `sudo chown root jping`

## IP Range Discover

Select the IP Range tab in the Discover window (**Tools > Discover**) to perform a discover based on one or more IP address ranges.

At the top of the tab is a table where you specify the IP address ranges. Each row defines a single range. When you first open the tab, a default range is displayed based on the IP address of the Console workstation. To add a new range, right-click on an existing row and select Insert Row. A new row will be created above the selected row using the same parameters. To edit a range, simply tab through the parameters and either enter a new value or use the drop-down list to select a value. Tabbing past the last row will also create a new row. To perform the discover operation, enable the desired IP ranges and click the **Discover** button. (For more information, see [How to Discover Devices](#).)

---

**NOTE:** When an IP Range Discover operation is initiated, all of the enabled rows are checked for validity. If any rows have invalid parameters, the Progress column for that row will alert you to the invalid entry.

---

Use Console's table options and tools to filter, find, sort, print, and export information in the table, and to customize table settings. You can access these Table Tools through a right-mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

The results of the discover process are displayed in the [Discover Results table](#). You can then save the discovered devices to the NetSight database where they are displayed in the left-panel tree.



**NOTES:** If the IP Range includes broadcast addresses (.0, .255, .127, .128, depending on the subnet mask), the addresses may be discovered as devices. To make the polling of devices in the Console tree as efficient as possible, these addresses should be removed and not saved to the database.

Saving devices from a discover that spans multiple subnets will populate the Device Groups in the left panel with multiple IP addresses (one for each primary/secondary address and /or router interface) for the same router. If this occurs, in the Device view of the Properties Tab for the **All Devices** group, sort the table on the **Base MAC** column, then scan that column, looking for multiple entries of the same MAC address. When you find multiple entries, you may choose to delete all but one or use the Table Editor in the Access View to set the **Poll Type** column for all but one interface to **Not Polled**, thereby reducing polling traffic. You can also use the [Hide Duplicate and Empty MACs checkbox](#) in the Discover Results Table to filter out duplicate entries prior to saving the devices.

NetSight Discover: IP Range

IP Range CDP Seed IP

To add or delete rows from this table, use the right-click menu, tab or arrow keys. If a device is discovered via multiple rows, the settings of the row with the lowest numbered Precedence will be used.

Enabled	Precedence	Start IP	End IP	Profile	Context	Poll Type	Poll Group	Vendor	Progress
<input type="checkbox"/>	1	10.20.10.1	10.20.10.254	public_v1_Profile	< None >	SNMP	Default	All	Disabled
<input checked="" type="checkbox"/>	2	10.20.20.1	10.20.20.254	public_v1_Profile	< None >	SNMP	Default	All	100%

Options... Profile Details Discover

Hide Duplicate and Empty MACs

Devices: (22)

IP Address	Display Name	Device Type	Base MAC	Status	Profile	Poll Type	Poll Group	Contact
10.20.20.15	10.20.20.15	Matrix N7 Gold	00:01:F4:7F:1F:D7	Exists	public_v1_Profile	SNMP	Default	QA Lab
10.20.20.14	10.20.20.14	6H202-24	00:00:1D:D4:D4:C1	New	public_v1_Profile	SNMP	Default	
10.20.20.11	10.20.20.11	6H252-17	00:E0:63:1D:B5:91	New	public_v1_Profile	SNMP	Default	contact2
10.20.20.10	10.20.20.10	6H352-25	00:E0:63:BC:85:64	New	public_v1_Profile	SNMP	Default	contact
10.20.20.9	10.20.20.9	6H308-24	00:E0:63:B6:F8:54	New	public_v1_Profile	SNMP	Default	contact
10.20.20.40	10.20.20.40	6H202-24	00:E0:63:A6:C0:04	New	public_v1_Profile	SNMP	Default	QA Lab
10.20.20.29	10.20.20.29	6H122-08	00:00:1D:8E:BF:E2	New	public_v1_Profile	SNMP	Default	QA Lab
10.20.20.1	10.20.20.1	ER-16	00:01:F4:05:23:1C	New	public_v1_Profile	SNMP	Default	

Export Remove Save All Close Help

254 IPs Queried, 254 Completed, 0 Outstanding, 22 Discovered Devices.

## IP Range Tab

Select this tab to perform a discover based on one or more IP address ranges. You must specify a range of IP addresses to be queried, and select a Profile that

---

will give the Discover tool read access to the devices you wish to discover.

---

**TIP:** Specify as narrow an IP address range as possible. The wider the range, the longer it will take to perform the discover. For example, if you are discovering IP addresses 111.111.111.20 through 30, and 111.111.111.240 through 250, it is faster to create two separate ranges rather than one range for 111.111.111.20 through 250.

---

### Enabled

Select the checkbox to enable Discover for the IP address range. Only enabled ranges will be searched when a discover operation is performed.

### Precedence

Precedence determines which parameters will be used if a device is in more than one range (the lower number yields higher precedence). For example, if a device is in two ranges -- one range with a precedence of 1 using an SNMPv3 profile, and one range with a precedence of 2 using an SNMPv1 profile -- the device will be saved with the SNMPv3 profile because that range has the higher precedence. The position of a row determines the Precedence of the range.

### Start IP

Enter the IP address at which the range should begin.

### End IP

Enter the IP address at which the range should end.

### Profile

Use the drop-down list to select the access Profile that will give the Discover tool read access to the devices you wish to discover. To create or edit a profile, click the **Profile Details** button to open the Authorization/Device Access Window - Profiles/Credentials Tab. If you discover an existing device using a different profile than the device is already using in the database, [saving](#) the device will overwrite the profile currently being used in the database. **Ping Only** allows discovering devices, such as workstations and other devices that are not configured for SNMP. If Ping Only is selected, the Poll Type must be set to **Ping**. (See the [Configuring Ping for Linux and Mac OS X Clients](#) section above.)

### Context

SNMP Context lets you specify a context that has been configured on a device. The context lets you access a subset of MIB objects related to that context. Console lets you specify a SNMP Context for both SNMPv1/v2 and SNMPv3.

---

The use of context differs depending on the protocol version being used with the credentials used by the selected **Profile**:

- When used with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.
- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, a SNMPv1 or SNMPv2 credential (community name) can be mapped through Local Management to a particular SNMP context on the device. When SNMPv1/v2 credentials are used with a Context entry, access is granted to the subset of MIB objects associated with that context. If the credential used is accepted, but the context specified doesn't match a context configured on the device, access is granted to the default context.

Console treats each context for a given device (IP address) as a distinct device. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to your device *Configuration Guide* for more information about setting and showing SNMP contexts.

### Poll Type

Use the drop-down list to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the [Profile](#) specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. If you discover an existing device using a different poll type than the device is already using in the database, [saving](#) the device will overwrite the poll type currently being used in the database.

---

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

---

### Poll Group

Use the drop-down list to select a Poll Group for the discovered devices. Console provides three distinct poll groups (defined in the Status Polling view of the Options window) that each specify a unique poll frequency. When you save newly discovered devices to the database, they will be polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

---

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

---

### Vendor

Use the drop-down list to specify whether you want to discover all devices or only Extreme Networks devices.

### Progress

This column displays the progress of the discover operation as a percentage or a status message. For example, if the row is not enabled, this column will display "Disabled" or when the row contains an invalid discover argument "Error-Invalid" is displayed.

### *Right-click Menu*

Right-clicking anywhere in the IP Range table displays a menu with the table options discussed in the Table Tools Help topic, plus the following four menu options:

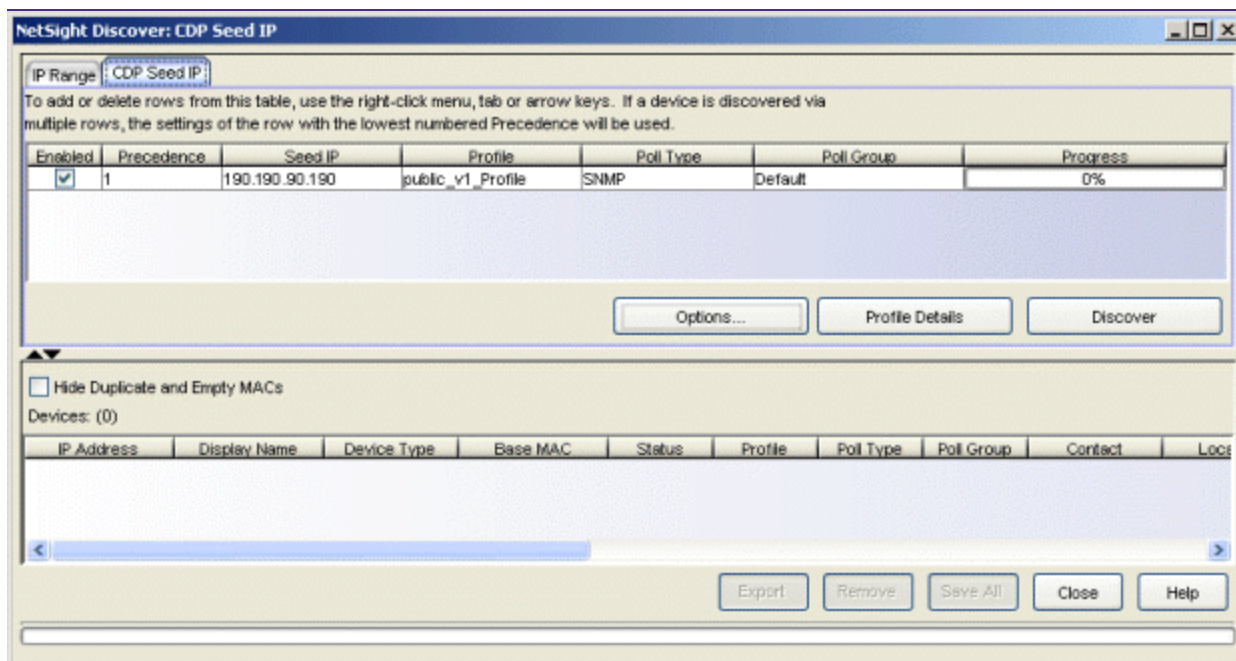
- **Enable Selected Row(s)** -- Enables all rows selected in the table. Only enabled rows (ranges) are searched when a discover operation is performed.
- **Disable Selected Row(s)** -- Disables all rows selected in the table. Disabled rows (ranges) are not searched when a discover operation is performed.
- **Insert Row** -- Creates a new row prior to the selected row with a range based on the IP address of the Console workstation and default values for the remaining parameters.
- **Delete Row(s)** -- Deletes the selected rows from the table.

## CDP Seed IP Discover

Select the CDP Seed IP tab in the Discover window (**Tools > Discover**) to perform a discover for CDP-compliant devices. The results of the Discover process are displayed in the [Discover Results table](#). You can then save the discovered devices to the NetSight database where they are displayed in the left-panel tree.

**NOTES:** Saving devices from a discover that spans multiple subnets will populate the Device Groups in the left panel with multiple IP addresses (one for each primary/secondary address and /or router interface) for the same router. If this occurs, in the Device view of the Properties Tab for the **All Devices** group, sort the table on the **Base MAC** column, then scan that column, looking for multiple entries of the same MAC address. When you find multiple entries, you may choose to delete all but one or use the Table Editor in the Access View to set the **Poll Type** column for all but one interface to **None**, thereby reducing polling traffic. You can also use the [Hide Duplicate and Empty MACs checkbox](#) in the Discover Results Table to filter out duplicate entries prior to saving the devices.

When you save newly discovered devices to the database, they will be polled with the default poll group designated in the Status Polling view of the Options window. If you save discovered devices that already exist in the database, the default poll group will overwrite the poll group currently being used in the database.



### *CDP Seed IP Tab*

Select this tab to perform a discover based on a CDP Seed IP address. You must specify a CDP seed device, and select a Profile that will give the Discover tool read access to the devices you wish to discover. Discover initiates contact with the seed device, and begins discovering all CDP-compliant devices, starting with the device's CDP Neighbor Table.

#### **Enabled**

Select the checkbox to enable Discover for the CDP Seed IP discover. Only enabled rows will be searched when a discover operation is performed.

## Precedence

Precedence determines which parameters will be used if a device is in more than one range (the lower number yields higher precedence). For example, if a device is in two ranges -- one range with a precedence of 1 using an SNMPv3 profile, and one range with a precedence of 2 using an SNMPv1 profile -- the device will be saved with the SNMPv3 profile because that range has the higher precedence. The position of a row determines the Precedence of the range.

## Seed IP

Enter the IP address for your CDP seed device.

---

**NOTE:** If CDP is not enabled on a seed device, a message is displayed, asking if you would like to enable CDP. **Yes** enables CDP in the device, waits for 30 seconds, then continues with the discovery. **No** cancels discovery using that seed device.

---

## Profile

If you are using a Seed IP address:

Use the drop-down list to select the access Profile that will give the Discover tool read access to the devices you wish to discover. To create or edit a profile, click the **Profile Details** button to open the Authorization/Device Access Window - Profiles/Credentials Tab. If you discover an existing device using a different profile than the device is already using in the database, [saving](#) the device will overwrite the profile currently being used in the database.

## Poll Type

Use the drop-down list to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the [Profile](#) specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. (See the [Configuring Ping for Linux and Mac OS X Clients](#) section above.) If you discover an existing device using a different poll type than the device is already using in the database, [saving](#) the device will overwrite the poll type currently being used in the database.

---

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

---

## Poll Group

Use the drop-down list to select a Poll Group for the discovered devices. Console provides three distinct poll groups (defined in the Status Polling view of the Options window) that each specify a unique poll frequency.

When you save newly discovered devices to the database, they will be polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

### Progress

This column displays the progress of the discover operation as a percentage or a status message. For example, if the row is not enabled, this column will display "Disabled" or when the row contains an invalid discover argument "Error-Invalid" is displayed.

## Discover Results Table

This table displays results from your discover operation. Use Console's table options and tools to filter, find, sort, print, and export information in the table, and to customize table settings. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body.

### Hide Duplicate and Empty MACs checkbox

Checking this checkbox filters the Discover Results table to show one discovered device per MAC address. When routed interfaces cause the same device to be discovered multiple times, use this checkbox to filter out duplicate entries.

### IP Address

The IP address of the device.

### Display Name

The device name that will be displayed in Console's left-panel tree. There are three types of display names:

- **IP Address** -- the device's IP address.
- **System Name** -- the administratively-assigned name of the device taken from the *sysName* MIB object.
- **User Defined Nickname** -- as defined in the Device Properties Tab. Select your preferred display name type in the .

### Device Type

The type of device.

**Base MAC**

The base MAC address for the device.

**Status**

Displays whether the discovered device is newly discovered (New) or already part of the NetSight database (Exists).

**Profile**

The access profile used to discover the device. If you discover an existing device using a different profile than the device is already using in the database, [saving](#) the device will overwrite the profile currently being used in the database.

**Poll Type**

The poll type used to discover the device: SNMP, Ping or Not Polled. For CDP Seed IP Discovers, the Poll Type is always SNMP or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified in the discover operation. If you discover an existing device using a different poll type than the device is already using in the database, [saving](#) the device will overwrite the poll type currently being used in the database.

**Poll Group**

Console provides three distinct poll groups that each specify a unique poll frequency. IP Range Discovers allow you to specify the desired poll group when you create the range. CDP Seed IP Discovers use the default poll group designated in the Status Polling view of the Options window. When you save newly discovered devices to the database, they are assigned to the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here will overwrite the poll group currently being used in the database.

---

**NOTE:** If a Poll Type of "Not Polled" is specified, the Poll Group will only be used if/when the Poll Type is changed to SNMP or Ping.

---

**Contact**

The contact person for the device based on the device's *sysContact* MIB attribute.

**Location**

The physical location of the device based on the device's current *sysLocation* MIB attribute.

**Firmware**

The current firmware version running in the device.



**Boot PROM**

The current boot PROM version running in the device.

**Uptime**

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

**Chassis**

The part number of the chassis where the device resides.

**Chassis Type**

The type of chassis where the device resides.

**Chassis ID**

The ID assigned to the chassis where the device resides. This is usually a serial number or MAC address, depending on the chassis type.

**Description**

Description of the piece of equipment, including its manufacturer, model number, and firmware version number. Ping-only devices such as printers or end stations will display Ping Only in this field.

**Options Button**

Opens the Discover Options window where you can set Discover SNMP options and table colors. These options can also be accessed from the Console Options window (Tools > Options).

**Profile Details Button**

Opens the Authorization/Device Access Window - Profiles/Credentials Tab where you can create and edit Console profiles.

**Discover Button**

Starts the Discover process.

**Export**

Exports the Discovered Devices table to an HTML file or a text file.

**Remove**

Removes the selected device(s) from the Discovered Devices table. This allows you to remove discovered devices that you do not want to save to the NetSight database.

**Save/Save All Button**

When one or more devices are selected in the table, the **Save** button saves the selected devices to the NetSight database. When no devices are

selected in the table, the **Save All** button saves all devices listed in the table to the NetSight database.

### *Status Bar*

The Status bar shows the progress of the current discovery.

### **IPs to Query/IPs Queried**

During a discover, this count shows the number of queries to be completed. Following a discover, the count shows the number of queries performed. IP Range Discovers query each device in the range once, but CDP Seed IP Discovers make two queries for each device so, for CDP Seed Discovers, this number will be twice the number of devices.

### **Completed**

Queries already performed.

### **Outstanding**

Queries to be performed.

### **Discovered Devices**

The number of devices discovered.

### *Right-click Menu*

Right-clicking anywhere in the Discovered Devices table displays a menu with the table options discussed in the Table Tools Help topic, plus the following menu options:

- **Remove** -- Deletes selected rows from the table.
- **Save** -- Saves the selected rows.
- **Add Devices to a Group** -- Opens the [Add Devices to a Group](#) window where you can specify a group where the selected devices will be saved. range based on the IP address of the Console workstation and default values for the remaining parameters.
- **Add to CDP Seed** -- Adds the selected rows to the CDP Seed IP table to be used as seed devices in a discover operation.
- **Select All** -- Select all rows in the table.

---

### **Related Information**

For information on related tasks:

- [How to Discover Devices](#)
- [Setting Discover Options](#)

## Edit Action Overrides Window

---

This window lets you override the default content contained in an alarm action message. For example, if you are creating an email action, you can customize the information contained in the email subject line and body. If you are creating a syslog or trap notification action, you can specify certain information that you want contained in the syslog or trap message.

The default message content that appears in the window (as shown below) is defined in the Suite-Wide Alarm Configuration options (Tools > Options > Suite > Alarm Configuration). Any overrides of the default content that you make here will only affect the specific alarm action that you are editing.

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. See below for a list of available keywords, along with their definitions.

The Custom Arguments field is used to specify the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as \$keyword. A group of literals and variables can be combined into a single argument by using double quotes. The value "all" is a special value that tells NetSight to pass all variable values to the program as individual arguments.

To access this window, select the Override Content checkbox in the Actions subtab in [Alarms Manager window](#), and click the **Edit Content** button.

## Keyword Definitions

There are certain \$keywords that you can use as variables in your alarm action messages. These \$keywords are replaced with information from the alarm when the alarm action is executed. Following is a list of available \$keywords, along with the value the \$keyword will return.

### Alarm Keywords

\$alarmName	The name of the alarm.
\$alarmSource	The component (such as a device) that raised the alarm.
\$alarmSourceName	The value varies depending on the alarm source: <ul style="list-style-type: none"> <li>• For a device or entity with an IP address, it will be the resolved host name of the alarm source. The NetSight Server must be able to resolve the alarm source IP address to a host name (DNS, hosts file) and the Alarm/Event Logs and Tables &gt; Resolve source host names option must be enabled in the Suite-Wide options (Tools &gt; Options).</li> <li>• For an AP serial number, it can be the AP name.</li> <li>• Other alarm sources may provide different source names.</li> <li>• If no alarm source name is available, the string will be empty (blank).</li> </ul>
\$alarmSubcomponent	The subcomponent (such as an interface) that raised the alarm.
\$severity	The alarm <a href="#">severity</a> .

<b>Alarm Keywords</b>	
\$type	The value returned is always "Alarm".
\$trigger	Indicates whether the trigger was a trap or event.
\$server	The NetSight server IP address.
\$time	The date and time when the event or trap occurred.
\$message	The event message.
\$eventType	The event type (event or trap).
\$eventSeverity	The event severity.
\$eventCategory	The event category.
\$eventTitle	The event message.
\$deviceIP	The IP address of the device that is the source of the alarm.
\$deviceIpCtx	The device IP and Context.
\$deviceNickName	The device nickname.
\$deviceBootProm	The BootProm version on the device.
\$deviceFirmware	The firmware version on the device.
\$deviceStatus	The device status.
\$snmp	The device SNMP credentials
\$sysName	The system name.
\$sysLocation	The system location.
\$sysContact	The system contact.
\$sysDescr	The system description
\$sysUpTime	The system uptime.
\$chassisId	The chassis ID.
\$chassisType	The chassis type.
\$trapName	The trap name.
\$trapEnterprise	The Enterprise for this trap (Extreme, snmpTraps, rmonEventsV2, dot1dBridge) as defined in the trapd.conf file.
\$trapOid	The trap OID.
\$trapArgs	The trap arguments.
\$trapArg{1-8}	Nth Trap argument.

## Related Information

For information on related windows:

- [Alarms Manager Window](#)

## Edit Custom Alarm Criteria Window

Alarms are triggered when certain trap or event conditions occur on your network. This window lets you define very specific criteria to trigger an alarm.

Each option lets you select one or more attributes to match against in the trap or event, in order to trigger the alarm. For each option, if you check the **Match On** box, then Alarms Manager filters based on that category. If you don't check the **Match On** box, then Alarms Manager doesn't filter based on that category, and as a result matches everything. However, if you don't check any **Match On** boxes, then Alarms Manager won't match any trap or event.

Configure the criteria to match for this alarm.

Match on Severity

Match Selected  
 Exclude Selected

Selected	Severity
<input type="checkbox"/>	Alert
<input type="checkbox"/>	Critical
<input type="checkbox"/>	Emergency
<input type="checkbox"/>	Error
<input type="checkbox"/>	Info
<input type="checkbox"/>	Notice
<input type="checkbox"/>	Warning

Match on Category

Match Selected  
 Exclude Selected

Selected	Category
<input type="checkbox"/>	Application
<input type="checkbox"/>	Database
<input type="checkbox"/>	Discover
<input type="checkbox"/>	Error
<input type="checkbox"/>	FlexView
<input type="checkbox"/>	HVDC
<input type="checkbox"/>	Lock
<input type="checkbox"/>	MSTP

Match on Type

Match Selected  
 Exclude Selected

Selected	Type
<input type="checkbox"/>	Event
<input type="checkbox"/>	Inform
<input type="checkbox"/>	Trap

Match on Event

Match Selected  
 Exclude Selected

Selected	Event
<input type="checkbox"/>	Alarm Threshold Exceeded
<input type="checkbox"/>	Application Shutdown
<input type="checkbox"/>	Application Started
<input type="checkbox"/>	Authentication
<input type="checkbox"/>	Authorization
<input type="checkbox"/>	CDP Neighbor Not Discovered
<input type="checkbox"/>	Contact Established
<input type="checkbox"/>	Contact Lost

Match on Host or IP/Subnet

Match Selected  
 Exclude Selected

Edit List...

Selected	Type	Host or Subnet
<input type="checkbox"/>	Host Name	10.20.30.40
<input type="checkbox"/>	IPMask	11.22.33.44/32
<input type="checkbox"/>	Host Name	iswordfish

Match on Log Manager

Match Selected  
 Exclude Selected

Selected	Log Manager Name
<input type="checkbox"/>	Policy
<input type="checkbox"/>	Syslog
<input type="checkbox"/>	Traps
<input type="checkbox"/>	adminEvent
<input type="checkbox"/>	asm
<input type="checkbox"/>	console
<input type="checkbox"/>	Inventory
<input type="checkbox"/>	nonAnnounceEvent

Match on Information Text

Match Any Selected  
 Match All Selected

Edit List...

Selected	Match Phrase	Contains Phrase
----------	--------------	-----------------

OK Cancel Help



### Match on Severity

Select one or more event severity levels to match against.

- **Match Selected** - The reported Severity is matched against any of the Severity levels selected in the list.
- **Exclude Selected** - The reported Severity matches if it is not one of the Severity levels selected in the list.

### Match on Category

Select one or more event categories to match against the Category column of the event. An event category is a way to group related events. For example, all events related to device discovery would be in the "Discover" category.

- **Match Selected** - The reported Category is matched against any of the categories selected in the list.
- **Exclude Selected** - The reported Category matches if it is not one of the categories selected in the list.

### Match on Type

Select one or more message types (Event, Inform, Trap) to match against the Type column of the event.

- **Match Selected** - The reported Type is matched against any of the types selected in the list.
- **Exclude Selected** - The Type matches if it is not one of the message types selected in the list.

### Match on Event

Select one or more event types to match against the Event column of the event.

- **Match Selected** - The reported Event is matched against any of the event types selected in the list.
- **Exclude Selected** - The reported Event matches if it is not one of the event types selected in the list.

### Match on Host or IP/Subnet

Select one or more host names or IP/Subnet addresses to match against the value of the address appearing in the Source column of the event. The list of host names and IP/ Subnet addresses can be edited by clicking the **Edit List** button to open the [Match Host window](#).

- **Match Selected** - The reported host name or IP/Subnet address is matched against any of the host or IP/Subnets selected in the list.
- **Exclude Selected** - The reported host name or IP/Subnet address matches if it is not one of the host or IP/Subnets selected in the list.

#### Match on Log Manager

Select one or more Event Logs to match against.

- **Match Selected** - The log where the event was received is matched against any of the logs selected in the list.
- **Exclude Selected** - The log where the event was received matches if it is not one of the logs selected in the list.

#### Match on Information Text

Select one or more text strings (phrases) to match against the text in the Information column of the event or trap. The list of text phrases can be edited by clicking the **Edit List** button to open the [Match Phrase List window](#).

- **Match Selected** - The Information text string is matched against one or more phrase selected from the list.
- **Exclude Selected** - The information text string matches if it is not one of the phrases selected from the list.

---

### Related Information

For information on related windows:

- [Alarms Manager Window](#)
- [Match Host IP or Subnet List](#)
- [Match Phrase List](#)

For information on related tasks:

- [How to Configure Alarms](#)
- [How to Configure Custom Alarm Criteria](#)

## Edit Flow Criteria Window

Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. NetFlow is a flow-based data collection protocol that provides information about the packet flows being sent over a network. K-Series, S-Series, and N-Series devices support NetFlow flow collection. For more information about NetFlow, see the [Flow Sensor Configuration Window](#) Help topic.

Use the [Alarms Manager window](#) to create your flow alarm definition, and then use this window to identify the flow criteria that must be matched to trigger a flow alarm.

When creating flow alarms, be aware that NetSight might handle thousands of flows each second, and performance can degrade if there are too many flow alarms configured, or if the configured flow alarms match too many flows.

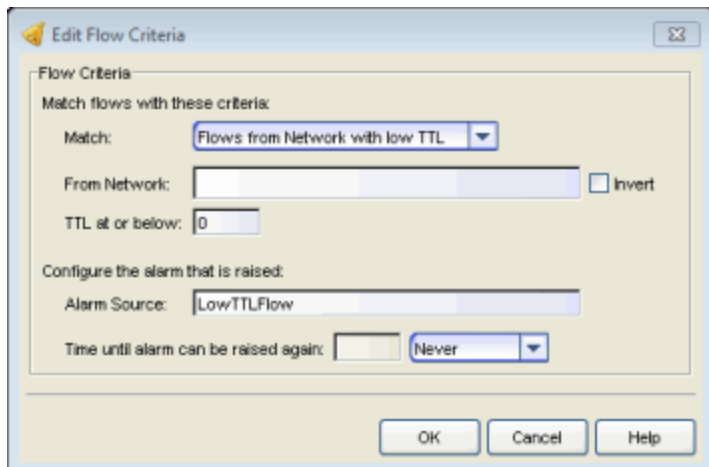
Here are two examples of how flow alarms can be useful on the network:

- Flow alarms can provide visibility of users with multiple devices hidden behind NAT gateways, by detecting network traffic with low TTL (IP Time to Live) values. This detection is based on the TTL field contained in the IP header of a frame. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. So, for example, if a packet from a Windows machine with a default TTL of 128 is detected by NetFlow with a TTL of 127, then it can be deduced that the packet has traversed a routed interface or NAT gateway, and an alarm can be triggered.
- Flow alarms can be used to detect suspicious or undesirable network traffic. This detection is based on the flow's source or destination IP address and (optional) port number. For example, flows from an internal or external web server, or flows from a web server to an external IP address, can be detected and cause an alarm to be triggered.

---

**NOTE:** There is no way to clear Flow alarms automatically. You can create an action-only alarm ([Alarms Manager window, Other Options tab](#)) to avoid the need to manually clear a Flow alarm.

---



## Match

Use the drop-down menu to select the way the flow is matched for a flow alarm to be triggered, and then specify the corresponding values in the fields below.

- Flows from Network - Match a flow's source IP address to the specified network.
- Flows to Network - Match a flow's destination IP address to the specified network.
- Flows from Network from Port - Match a flow's source IP address and port number to the specified network and port.
- Flows from Port to Network - Match a flow's source port number and destination IP address to the specified port and network.
- Flows from Network with low TTL - Match a flow's source IP address and TTL value to the specified network and the "TTL at or below" value.

## From/To Network

A network is identified as a set of IP masks. The mask is used as a filter to define a range of IP addresses. Masks can be entered in CIDR or dotted-decimal format.

- **CIDR** - CIDR format uses a slash followed by a number between 8 and 32, to define the number of contiguous, left-most "one" bits that define the network mask. For example, /16 indicates a 16-bit mask. Here is an example of a From/To Network value using the CIDR format:  
10.20.30.0/16,10.20.80.0/24

- **Dotted-Decimal** - Dotted decimal format represents network masks as four octets separated by periods. For example, a 16-bit mask in dotted decimal notation is *255.255.0.0*. Here is an example of a From/To Network value using the dotted-decimal format:  
10.20.30.0/255.255.0.0,10.20.88.0/255.255.255.0

For example, if you entered either 10.20.0.0/16 (CIDR) or 10.20.0.0/255.255.0.0 (Dotted-Decimal) in the From/To Network field, then all incoming packets in the range 10.20.00.00 through 10.20.255.255 would result in an address match.

If you select the **Invert** checkbox, it will be considered a match if the flow criteria does **not** match the specified values.

#### **From Port**

Enter the port number to be matched.

#### **TTL at or below**

If the TTL value in the packet's TTL field is equal to or less than the value entered here, then the TTL criteria is a match.

#### **Alarm Source**

Enter a phrase to be used as the source of the alarm, when the alarm is raised.

#### **Time until alarm can be raised again:**

Use this field to configure time-based suppression of the flow alarm. Once the alarm is triggered, it will not be triggered again until the specified time has passed. This prevents a large number of alarms being triggered, if many flows match the alarm criteria. If you select "Never", the alarm will only trigger one time. Once you manually clear the alarm, it can be triggered again.

---

### **Related Information**

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)

## Edit Threshold Window

A threshold alarm is a network alarm that is triggered when a specified value enters an unacceptable range, for example, when CPU utilization exceeds 80% or when an application exceeds 10 GB in an hour. The Edit Threshold window lets you define the threshold value that will be used to trigger a threshold alarm.

Use the [Alarms Manager window](#) to create your threshold alarm definition, and then use this window to identify the type of threshold, select the statistic to monitor, and specify the threshold value that triggers the alarm.

There are two threshold alarm types: OneView and Application Analytics. A OneView threshold alarm is based on reporting data monitored by the OneView Collector. A Application Analytics threshold alarm is based on application usage data collected on the Application Analytics engine.

You must have statistics collection and flow collection enabled for your network devices in order to collect the data used to determine whether a threshold has been passed. See [Enable Report Data Collection](#) and [Enable Flow Collection](#) in the Management Center Getting Started Help topic for instructions. To use Application Analytics threshold alarms, you must be using Application Analytics.

For information on how to clear OneView and Application Analytics alarms, see [How to Clear Threshold Alarms](#).

## OneView Threshold Alarm

The OneView Collector gathers historical reporting data over time, which is then used in Management Center reports. Threshold alarms are raised when the reporting data matches a threshold alarm criteria.

**Edit Threshold**

Threshold Configuration  
Configure the threshold for this alarm.

Threshold Type: OneView

OneView Threshold

Statistic Type: Interface

Statistic Name: Interface % Availability

Statistic Description:  
Interface % Availability. Source: ifAdminStatus + ifOperStatus

Minimum value: 0.0 Maximum value: 100.0

Cross when value goes below 50.0

Rearm when value goes above 80.0

OK Cancel Help

### Threshold Type

Select **OneView** as the threshold type.

### Statistic Type

Select the type of statistic to monitor.

### Statistic Name

Select the statistic to monitor. The list of statistics varies depending on the Statistic Type that is selected. See a description of the selected statistic in the field below the statistic name.

### Statistic Description

A description of the selected statistic is displayed, as well as the source of the statistic.

### Minimum/Maximum value

The minimum and maximum values allowed for the selected statistic (if applicable).

### Cross when value

Select the crossing direction and specify the statistic value. A rising threshold triggers the alarm when the statistic goes above the specified value. A falling threshold triggers the alarm when the statistic goes below the specified value. If you're configuring a clearing alarm, specify the value that clears the alarm here.

### Re-arm when value goes below

If you select the re-arming checkbox, the threshold alarm will clear itself when the monitored statistic is restored to an acceptable range. When an alarm self-clears, no action is triggered. Enter a value that will be used to determine when the threshold alarm will clear itself. The value should be close, but not too close, to the threshold value. If the value is too close to the threshold value, then run-time values that hover around the threshold value can trigger and clear alarms too frequently, resulting in noisy alarm activity.

## Application Analytics Threshold Alarm

The Application Analytics engine generates Application Analytics threshold alarms as part of the application usage collection process. Threshold alarms are raised when hourly or high-rate usage data matches a threshold alarm criteria. Each target record produced on the Application Analytics engine is evaluated at the end of each collection interval to see if it matches alarm criteria. If a statistic has crossed a configured threshold, an alarm is raised.

Alarms can track single target types as well as target combinations. They can reference specific targets, for example a specific application such as Facebook, or they can reference all the targets in a target type, for example all applications. Only the target types and target combinations that are collected by Application Analytics can be used in alarms.

Here are some examples of possible Application Analytics threshold alarms:

- Raise an alarm when the BitTorrent application exceeds 10 GB in an hour.
- Raise an alarm when any iOS application exceeds 1 GB uploaded in an hour.
- Raise an alarm when any client uses more than 50 applications in a 5-minute interval.
- Raise an alarm when there are more than 10,000 servers detected in an hour.
- Raise an alarm when the Outlook application's average response time is more than 5 seconds in an hour.



## Threshold Type

Select Application Analytics as the threshold type.

## Collector

Application Analytics application usage data is collected in hourly and in high-rate (five-minute) intervals. Set the collector to use the interval that you would like data checked. Some target types are not available when the high-rate collector is selected.

---

**NOTE:** Application Analytics hourly threshold alarms are not triggered until the hourly calculation, and high-rate threshold alarms are not triggered until the end of the high-rate interval. For example, if there is excessive network usage at 3:05, the hourly threshold alarm will not be triggered until the hourly total is calculated at 4:00.

---

## Target Type

Select the target type that you want the alarm to monitor. Options includes single targets as well as target combinations. Only the target types that are collected by Application Analytics can be used in alarms.

Depending on the target type you select, you can choose to limit the alarm testing to a specific target instance by entering a target name in the

applicable field, or you can test for all instances by selecting the "Any" checkbox.

Alarms will be raised for all targets that match the alarm. The name of the specific target that matched will be included in the alarm message.

- **Applications** - An application identified in Application Analytics, such as Facebook.
- **Application Groups** - Application categories, such as Cloud Computing or Social Networking.
- **Clients** - The end-point of a flow which has the client role for that connection.
- **Servers** - The end-point of a flow which has the server role for that connection.
- **Locations** - The network location for the client of an application flow. For more information, see [Network Locations](#).
- **Device Families** - The kind of device determined for a client, such as Windows or iOS.
- **Profiles** - A profile assigned to a client.
- **Application/Client** - Information about applications used by clients, or about clients using an application.
- **Application/Device Family** - Information about applications used by device families.
- **Application/Profile** - Information about application use within a profile.
- **Total** - The total accumulated statistics for the interval, collected from all network flows (with the exception of client count, server count, and application count statistics, which are collected from in-network flows).
- **Total - All Flows** - Client count and server count statistics collected from all network flows.

### Statistic

Select the statistic that you want the alarm to monitor. Options vary depending on the selected target type. The final statistic value at the end of the interval is what is tested against the threshold value.

- **Bytes** - The number of bytes transferred in both directions, between the client and the server. Also known as bandwidth. You can track sent and received bytes as well as total bytes. Examples:  
Facebook exceeds 100 MB in an interval.  
Any client exceeds 100 MB uploaded in an interval.

Any client exceeds 1 GB downloaded in an interval.

- **Flows** - The number of NetFlow records sent by the switch to report the traffic between the client and the server. You can track inbound and outbound flows as well as total flows. Example:  
Any client has at least 1 BitTorrent flow.
- **Clients** - The number of unique clients associated with the target. Example:  
There are more than 10 clients in profile "Unregistered Guests".
- **Servers** - The number of unique servers associated with the target.  
Example:  
There are more than 10,000 servers detected in an hour.
- **Applications** - The number of unique applications associated with the target. Example:  
A client uses more than 50 applications in a 5-minute interval.
- **Network Response Time** - The average amount of time to create a connection. Example:  
Any location has an average network response time of 10 seconds or more during an hour.
- **Application Response Time** - The average amount of time for a server to respond to a request. Example:  
Any application has an average application response time of 10 seconds or more during an hour.

### Cross when value

Select the crossing direction and specify the statistic value. A rising threshold triggers the alarm when the statistic goes above the specified value. A falling threshold triggers the alarm when the statistic goes below the specified value. If you're configuring a clearing alarm, specify the value that clears the alarm.

Alarm values for bytes are specified in megabytes and values for time are specified in seconds. Fractional values such as 0.5 megabytes or 0.5 seconds are allowed.

### Threshold Description

This section explains the threshold being configured.

### Engines

If you have multiple Application Analytics engines, the alarm threshold can be applied to one or more specific engines or to all engines. Click the **Edit** button to open a window where you can select the desired engine(s). If no engines are selected, then the alarm threshold will be applied to all engines.

## Related Information

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)
- [How to Clear Threshold Alarms](#)

## E-Mail Configuration Window

---

The E-Mail Configuration window lets you create an e-mail recipient list to use when configuring e-mail actions. The window is accessed from the **Edit Mail Lists** button in the [Alarms Manager window](#) in the Actions subtab.

To create a new e-mail list, click the **New List** button and enter a name for the new list. In the E-Mail List Entries field, enter an e-mail address for each recipient you want on the list, separated by a comma or semicolon. These entries are the actual e-mail addresses (*username@domain*) of the intended recipients, separated by commas or semicolons. For example:

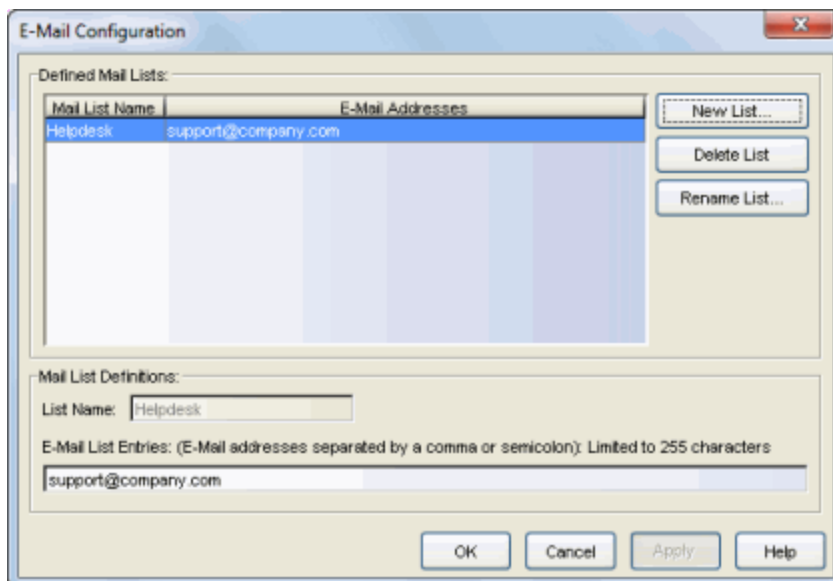
`thisuser@onecompany.com, thatuser@athome.net, etc.`

---

**NOTE:** Console does not verify this list for valid addresses.

---

To edit an e-mail list, select the list in the table, and then make your changes in the E-Mail List Entries field.



### Defined Mail Lists

Displays the currently defined mail lists. Use the **New List** button to create a new mail list.

### Mail List Definitions

Use the E-Mail List Entries field to configure the "send to" e-mail addresses for the selected list. Addresses in the list can be separated with a comma or

a semicolon. E-mail addresses must be entered in a valid email format, for example, jsmith@company.com.

**New List Button**

Opens a window where you can enter a new name for a mail list.

**Delete List Button**

Deletes the selected list.

**Rename List Button**

Lets you rename the selected list.

---

**Related Information**

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)

## Firmware Image Download Window

---

This window enables you to download a firmware image file to a device. You must have a TFTP Server running to perform the download operation. To access the Firmware Image Download window from the main Console window, right-click the device in the left panel and select **Firmware Image Download** from the menu. In Device Manager, select **Utilities > Firmware Image Download** from the Device View menu bar.

- 
- NOTES:**
1. Console does not support firmware download for the RoamAbout R2.
  2. This window is only available on devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.
-

The screenshot shows a window titled "Firmware Image Download: 10.20.30.40". It is divided into several sections:

- Current Device Settings:** Contains two text input fields. "Last Server IP:" is set to "10.20.31.51". "Last Filename:" is set to "\firmware\6000\50305.FLS".
- Operation:** Contains three radio buttons: "Download" (selected), "Download & Reset", and "Reset".
- Download Settings:** Contains several fields and buttons:
  - "TFTP Server IP:" is a dropdown menu set to "124.121.192.52 (local)".
  - A checked checkbox "Server uses Root Path:" is followed by a text field "C:\tftpboot" and a "Browse..." button.
  - "Full Image Path:" is a dropdown menu set to "\firmware\6000\50305.FLS (current)" with a "Browse..." button.
  - "Path to set on device:" is a text field containing "\firmware\6000\50305.FLS".
- Status:** Contains three text input fields:
  - "Operation Status:" is set to "Normal Operation".
  - "Error Description:" is empty.
  - "Bytes Transferred:" is empty.

At the bottom of the window, there are four buttons: "Apply", "Close", "Refresh", and "Help". Below the buttons is a section labeled "Current Values." which is currently empty.

## Current Device Settings

The information displayed in Current Device Settings varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

### Active Image File

Displays the location and filename of the active firmware image.



### Active Image Version

Displays the firmware image currently active in the device.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

### Last Server IP

Displays the IP address of the last TFTP server used.

### Last Filename

Displays the path and filename of the last image downloaded to the device.  
This is not necessarily the active firmware.

Devices that support *etsysConfigurationManagementMIB* do not provide values for these fields and will display "No Information Provided".

## Operation

Use the radio buttons to select the desired type of operation:

- **Download** -- Performs a download of the specified firmware image to the device. This operation will not activate the new firmware. A Reset operation must be performed to activate the downloaded image.
- **Download & Reset** -- Performs a download of the specified firmware image to the device and resets the device with the new image as soon as the download is complete.
- **Reset** -- Resets the device so that new firmware can be activated.

## Download Settings

Use this area to specify the download settings.

### TFTP Server IP

Enter the TFTP server's IP address, or use the dropdown list to select the TFTP server to perform the download operation. This list contains up to seven IP addresses: the IP address for the local workstation (local), the IP address of the TFTP server last set on the device (current), and up to five previously entered IP addresses. Greater than five addresses can be entered during a particular TFTP Download session, but only five are retained after this window is closed.

### Server Uses Root Path

If your TFTP server is configured with a root directory, select the checkbox and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which

the TFTP server is allowed access. The TFTP server will be allowed to download files from this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Suite-Wide Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

### Full Image Path

Enter the full path and filename of the image file you want to download to the device. You can also use the dropdown list to select a path and filename or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a [Root Path](#), the browse capability is limited to the directories below that root path.

### Path to Set on Device

This field displays the image path as it will be set on the device. If the [Server Uses Root Path](#) is selected, the specified root path is stripped from the full path and filename. If [Server uses Root Path](#) is not selected, this field displays the same path as the [Full Image Path](#) field.

## Status

The information displayed in Status varies depending on the device type.

---

**NOTE:** Devices that support *etsysConfigurationManagementMIB* will display dashes (--) in these fields until an operation begins, at which time they will report the progress of that operation.

---

### Operation Status

Displays the status of the download operation:

- **Normal Operation** -- following a download, indicates that the operation was completed successfully. Also indicates the device is operating within normal parameters.
- **Download Active** -- the device is currently processing a TFTP download.

- **Error Detected During Download** -- a download was started but an error was detected.
- **Other/Unknown** -- the device is in an unspecified or unknown state. For devices that support *etsysConfigurationManagementMIB*, the information is displayed as follows:
  - **Inactive** -- the device is currently not engaged in a transfer.
  - **Pending** -- the transfer operation is in queue.
  - **Running** -- the transfer operation is in progress.
  - **Success** -- the transfer operation completed successfully.
  - **Error Detected During Operation** -- an error occurred during the transfer.

#### **Error Description**

Displays a description of any error detected during a download.

#### **Bytes Transferred**

Depending on the device and the TFTP server being used, this field may display transfer statistics during a download operation. In some cases, a progress bar will also appear at the bottom of the screen (in the status bar), reporting the percentage of the download operation completed.

#### **Apply Button**

Sets the configured information to the device and starts the specified operation.

#### **Close Button**

Closes the window.

#### **Refresh Button**

Resets the fields to default values, as reported by the device.

---

### **Related Information**

For information on related tasks:

- [How to Download Firmware](#)

For information on related windows:

- [Configuration Upload/Download Window](#)

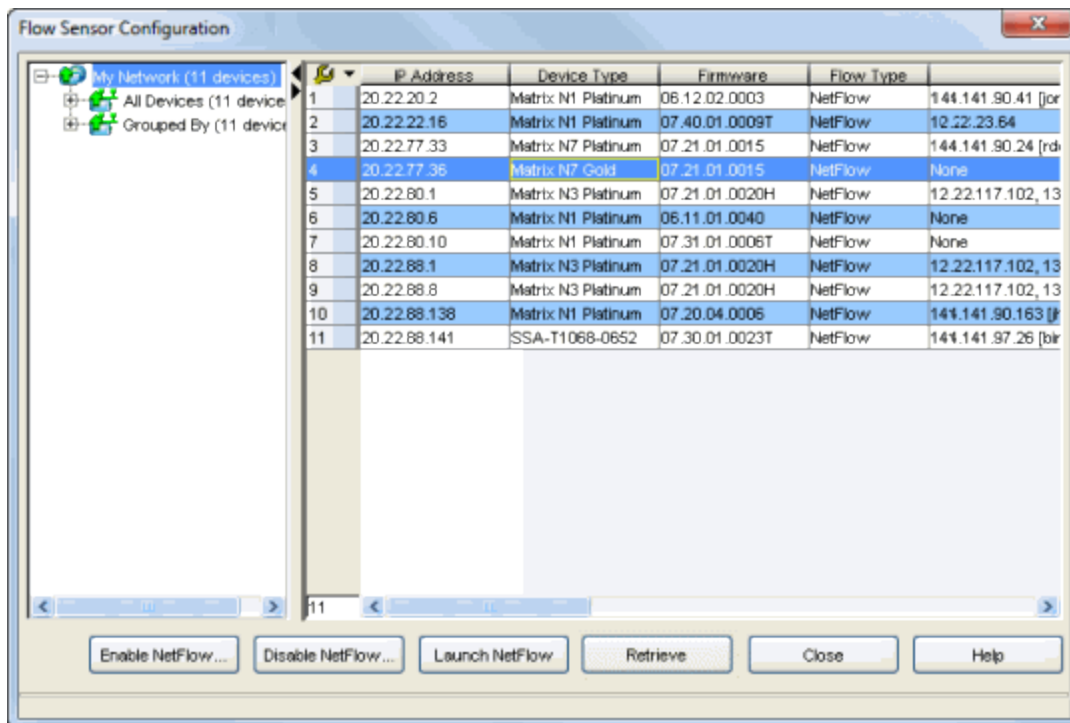
## Flow Sensor Configuration Window

The Flow Sensor Configuration window lets you enable or disable NetFlow on your network devices that support it. NetFlow is a flow-based data collection protocol that provides information about the packet flows being sent over a network. K-Series, S-Series, and N-Series devices support NetFlow flow collection.

You can access the window by selecting Tools > NetFlow Sensor Configuration from the Console menu bar. The window lists all the devices that support NetFlow. Click **Retrieve** to display all the devices in your network that support NetFlow, or click a device or folder in the tree to display information specific to those devices.

Select a device and use Enable NetFlow to add the NetSight server as a flow collector for that device. Up to four NetFlow collectors can be configured on a K-Series, S-Series, and N-Series device (firmware version 7.xx). However, only one collector can be configured on an N-Series device with firmware version 6.xx.

You must be a member of an authorization group that has been assigned the NetSight OneView > NetFlow Read/Write access capability in order to access this window.



**IP Address**

Device IP address.

**Device Type**

The type of device.

**Firmware**

The firmware version running on the device.

**Flow Type**

The type of flow collection supported by the device.

**Collector IPs**

The IP addresses of the flow collectors configured for this device. The device (flow sensor) will forward flow data to these addresses.

**Enabled Ports**

The ports on the device that have NetFlow enabled. Flow records for traffic travelling across these ports are forwarded to the collector IP addresses.

**Active Timeout**

For ongoing flows, a flow record is sent out at every interval of the active timeout. When NetFlow is configured by NetSight, this value is set to 1 minute. This means for a flow that lasts 2 minutes and 10 seconds, a flow record will be sent to the collectors three times for this flow: at the 1 minute mark, at the 2 minute mark, and when the inactive flow times out (40 seconds after it ends) at the 2 minute, 50 second mark. This is merged by the NetSight Flow Collector into a single 2 minute 10 second flow.

**Cache Status**

When configured by NetSight, the NetFlow cache is automatically enabled for the device. NetFlow records are stored in the NetFlow cache until the active timeout is triggered and the flow is sent to the collectors.

**NF Version**

The version of NetFlow records forwarded by the device to the collectors. Only version 9 is supported by NetSight. Flow records of any other version will be ignored.

**Template Timeout (v9)**

NetFlow Version 9 templates are resent after this timeout period (in minutes). The templates are used by the collectors to extract the v9 flow data. By default, this is set to 1 minute. The value can be changed in the [Console NetFlow options](#).

**Template Refresh (v9)**

NetFlow Version 9 templates are resent after this many flow packets. The templates are used by the collectors to extract the v9 Flow data. By default, this is set to 30 packets. The value can be changed in the [Console NetFlow options](#).

**Enable NetFlow**

Select a device and use Enable NetFlow to add the NetSight server as a flow collector for that device. To enable NetFlow on a port, it is recommended that you use PortView in Management Center. You can access PortView from the Console Port Properties tab or Interface Summary FlexView, by right-clicking one or more interfaces and selecting Port Tools > PortView.

**Disable NetFlow**

Select a device and use Disable NetFlow to disable NetFlow on that device. To disable NetFlow on a port, it is recommended that you use PortView in Management Center. You can access PortView from the Console Port Properties tab or Interface Summary FlexView, by right-clicking one or more interfaces and selecting Port Tools > PortView.

**Launch NetFlow**

Opens the **Flows** tab in Management Center, where you can see NetFlow diagnostic reports that let you analyze flow details, applications, senders, and receivers.

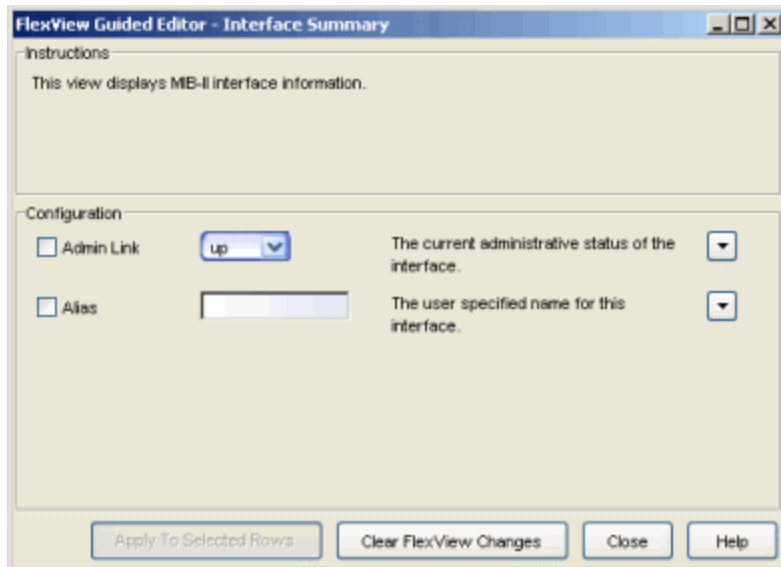
**Retrieve**

Click **Retrieve** to display all the devices in your network that support NetFlow.

## Guided Editor Window

---

You can use the Guided Editor to change the value in FlexView table columns that contain writeable MIB objects. Read the instructions in the top half of the window. Then, in the Configuration section, check the writeable objects that you are changing and enter the appropriate values as needed.



### Instructions

This area contains the instructions that were entered in the [FlexView Editing Instructions](#) field in the General tab of the FlexView Properties window.

### Configuration

This area lists all of the writable columns in the current FlexView and provides the appropriate facilities for editing their values together with column notes that were entered in the FlexView Properties.

### Apply to Selected Rows Button

This button enters the values that you've configured into the rows of the FlexView.

### Clear FlexView Changes Button

Serves to undo changes that have been applied to selected rows.

## Related Information

For information on related windows:

- [FlexView Properties Window](#)
- [FlexView Tabs](#)

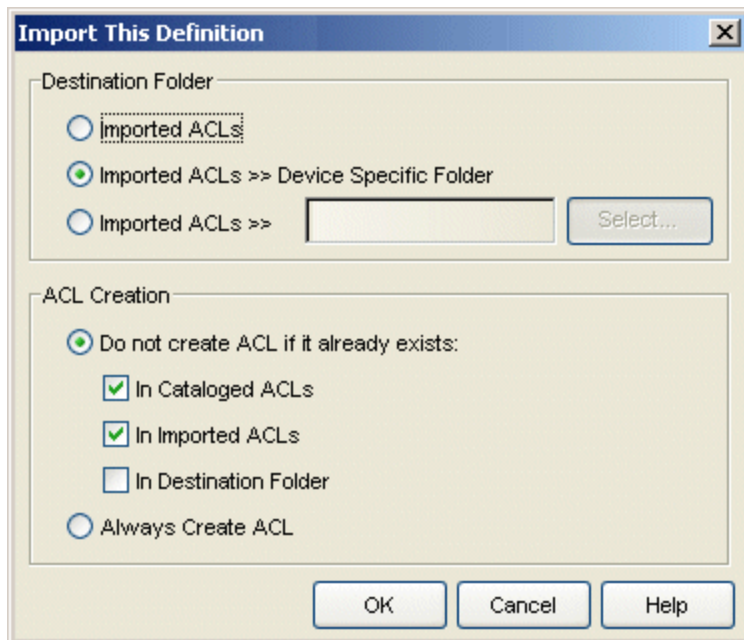
For information on related tasks:

- [How to Create and Modify FlexViews](#)
- [How to Use FlexViews](#)
- [How to Export the FlexView Catalog](#)



## Import This Definition Window

This window is accessed from the [ACL Verification Results window](#) and is used when copying the rules from the device ACL to the ACL in the ACL Manager database. Using the options in the window, you can control how the ACL data is handled during the import. The window lets you select a destination within the Imported ACLs folder and filter duplicate ACLs within specific folders.



### Destination Folder

Select from the following options:

- Imported ACLs - When selected, the imported ACL is placed in the Imported ACLs folder in the left-panel of the [ACL Editor](#).
- Imported ACLs >> Device Specific Folder - When selected, the imported ACL is placed in the appropriate device-specific folder in the left-panel of the ACL Editor.
- Imported ACLs >> <User-Defined Folder Name> - When selected, you can enter a folder name in the associated field, or use the **Select** button to select a folder within the Imported ACLs folder.

### ACL Creation

This area offers options to either filter out duplicate ACLs when importing, or always create the ACL regardless of duplications. The test for duplicate

ACLs can be further defined to compare imported ACLs to the ACLs in specific folders and sub-folders in the ACL Editor left-panel tree.

- Do not create ACL if it already exists - Compare and filter imported ACLs if a duplicate ACL exists in any of the selected folders. (Duplicate ACLs are ACLs that have the same name and the same rules.) You can select one or more folders. The imported ACLs are compared with ACLs in the selected folder(s) and all of its sub-folders. When **In Imported ACLs** is selected, the imported ACLs are compared with ACLs in the Imported ACLs folder and also in any more specific Destination Folders within the Imported ACLs folder.
  - Always Create ACL - No filtering occurs and the ACL is imported into the Destination folder specified.
- 

### Related Information

For information on related tasks:

- [How to Import ACL Data](#)

## Main Window

---

The Console Main Window serves as a control panel for accessing Console tools and functions and viewing Console information. It lets you monitor device status, define network configuration, and automate troubleshooting tasks. The main window is divided into six functional areas:

- [Menu Bar](#) - Functions, tools, and help available with Extreme Management Center (Management Center) Console
- [Toolbar](#) - Button shortcuts to frequently used menu selections.
- [Left Panel](#) - Devices modeled in the Management Center database
- [Right Panel](#) - Several tabs where you can use Console's FlexViews to examine the device/interface status and configure certain device settings, locate specific users and devices, and manage VLANs.
- Event View - Tables showing the alarms and events for Console and other Management Center applications.
- [Status Bar](#) - Operational status, errors and events

The Menus and Toolbar provide access to Console functions and other Management Center applications. The left panel contains the devices that have been modeled in the Management Center database. The right panel contains several tabbed views where you can create a map of the devices on your network, examine the device/interface status, locate specific users and devices, and manage VLANs. The bottom panel contains tables showing the alarms and events for Console and other Management Center applications.

### Sample Management Center Console Window

The screenshot displays the NetSight Console interface. The top menu bar includes File, Edit, Tools, Applications, and Help. Below the menu is a toolbar with various icons. The main window is divided into several sections:

- Left Panel:** A tree view showing the network structure under "My Network (97 devices)" and "All Devices (97 devices)". It lists various IP addresses such as 10.24.20.1, 10.24.22.10, 10.24.22.12, etc.
- Top Tab Bar:** Contains tabs for Welcome, Properties, Compass, VLAN, Basic Policy, ACL Manager, and Interface Summary. Below the tabs are radio buttons for Device, Access, Date/Time, and Port.
- Table 1 (Device List):** A table with columns: IP Address, Display Name, Device Type, Status, Firmware, Boot PROM, and Base MAC. It lists details for various devices, including their IP addresses, names (e.g., SSA-T4068-0252, A2H124-24P), types (e.g., Matrix N1 Platinum, Cisco 4507), and status (Contact Established).
- Table 2 (Event Log):** A table with columns: Acknowledge, Severity, Category, Timestamp, Source, Subcomponent, Client, User, Type, and Event. It shows a list of events, including database updates, device deletions, and user connections.
- Bottom Panel:** A console area with tabs for Console, Alarms, Traps, Syslog, Automated Security, Inventory, Policy Control Console, Policy, Scheduler, NAC, and Purview. It includes a progress indicator (0%) and an Alarms section showing 22 active alarms.

## Related Information

For information on related windows:

- [Menu Bar](#)
- [Toolbar](#)
- [Left Panel](#)
- [Right Panel](#)
- [Status Bar](#)

For information on related tasks:

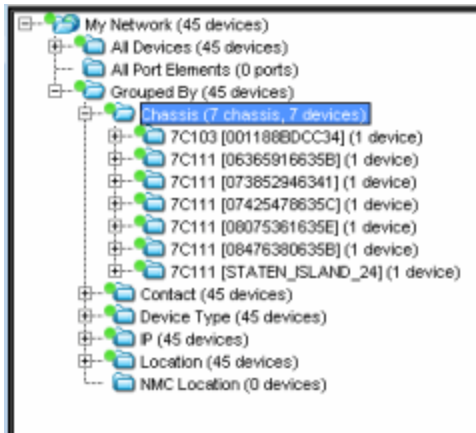
- [How to Add, Remove, and Rename Groups](#)
- [How to Add, Remove, and Delete Devices](#)

## Main Window Left Panel

---

The left panel contains a tree hierarchy showing all of the devices that have been modeled in the Extreme Management Center database. At the top of the hierarchy is the **My Network** branch, consisting of device groups containing the devices that you've modeled in Console.

### Sample Left (Tree) Panel



## My Network

This branch of the tree shows all of the devices that you've modeled in Console, either manually or through Discover, along with user-created groups.

### *System-Created Groups*

A fixed set of system-created groups, blue folders--that cannot be removed. These contain groups of devices:

- **All Devices** contains all of the devices modeled in the database.
- **All Port Elements** - Port Elements are used with FlexViews to query information specific to interfaces, bridge ports and other port types. Ports are added to the left panel by choosing **Add Port Elements to Group** from the right-click menu in a FlexView table.
- **Grouped By** contains sub-groups showing devices sorted according to Chassis, Contact, Device Type, IP address, and Location.

Devices are automatically added to the appropriate system created groups when they are added to Console. If devices are moved or for some other reason require an update to their grouping, you can use the **Reload Device Tree From Database** selection from the **My Network** right-click menu.

---

**NOTE:** Saving devices from a Discover that spans multiple subnets will populate the Device Groups in the left panel with multiple IP addresses (one for each router interface) for the same router. If this occurs, sort the table in the Properties Tab for the **All Devices** group on the **Base MAC** column, then scan that column, looking for multiple entries with the same MAC address. When you find multiple entries, you may choose to delete all but one or use the Table Editor to set the **Monitor** column for all but one interface to **None**, thereby reducing polling traffic.











---

### *User-created Groups*

You can create your own groups (user-created groups) according to the needs of your network. User-created groups can only be created in the My Network (top-level) group or in another user-created group. They can be nested to create a hierarchy of user-created groups

## Left Panel Icons

The following table defines icons that can appear in the left panel. For information about alarm/device status displayed in the device tree, see [Viewing Alarms](#).

Icon	Definition	Icon	Definition
	System-created Groups		User-created Groups
	Port Element		Switch
	Router		Wireless
	VPN		SNMP
	Pingable		Unknown

## Right-click Menus

Several right-click menus are available from a right-mouse click on icons in the left panel tree. The specific menu selections depends on the particular icon selected.

The following table describes the available menu selections.

<b>Menu Selection</b>	<b>Definition</b>	<b>Available From</b>
<b>Add Device</b>	Opens the Add Device window where you can define the IP address and community name for a device being added to the selected group.	My Network System-Created Groups User-Created Groups
<b>Add Device(s) to Group</b>	Adds the selected devices to a user-defined device group.	Devices
<b>Add Group</b>	Adds a Group to the selected group. Type a name, followed by Enter, to replace the highlighted (New Group) name.	My Network User-Created Group
<b>Copy</b>	Places a copy of the selected left panel object in the paste buffer.	My Network System-Created Groups User-Created Groups Devices
<b>Configuration Upload/Download</b>	Opens a Configuration Upload/Download window that you can use to retrieve configuration information from one device and download it to another device.	Device
<b>Contact Device using Groups Profile</b>	Attempts to contact the selected device(s) with the currently configured profile.	Device
<b>Copy</b>	Copies the selected object and places it in the paste buffer.	Devices, Device Groups
<b>Cut</b>	Removes the selected object from its current location in the left panel and places it in the paste buffer. If a subsequent Paste operation is not performed, the object is restored to its original location.	Devices in a User Created Group User-Created Groups
<b>Delete Device(s)</b>	Removes the selected device from the NetSight database.	Device
<b>Delete Device Group</b>	Removes the selected Group from the left panel.	User-Created Groups
<b>Delete Port Element</b>	Removes the selected Port Element from the left panel.	Port Element
<b>Device Manager</b>	Launches the Device Manager application for the selected device.	Device
<b>Execute Command Script</b>	Opens the NetSight Command Script tool that lets you execute a sequence of CLI commands (a script) on the selected devices.	Devices, Device Groups
<b>Expand/Collapse</b>	Shows/hides sub-groups nested within the selected group.	All except the lowest level, Device, etc.
<b>Firmware Image Download</b>	Launches the TFTP download utility for downloading firmware to devices.	Device
<b>MIB Tools</b>	Launches the MIB Tools utility.	Device



Menu Selection	Definition	Available From
<b>Import Device ACL Data</b>	Imports the existing ACLs from your devices into ACL Manager's ACL Editor.	Devices, Device Groups
<b>OneView</b>	Management Center (formerly OneView) will begin collecting data on the selected devices to use in its reports.	Devices
<b>Ping</b>	Launches the Ping Device window and initiates a ping of the selected device. <b>NOTE:</b> Ping requires membership in an Authorization Group that is granted administrative privileges.	Device
<b>Refresh (Rediscover)</b>	Attempts to contact the selected device(s) to update the properties information. Console uses the Profile for the Read Access Level of the NetSight Administrator's Authorization Group to refresh information.	Devices, Device Groups
<b>Refresh Device Data</b>	Refreshes the ACL assignment data for the devices' interfaces and agent services.	Devices, Device Groups
<b>Reload Device Tree From Database</b>	Reloads the device tree with the device data from the NetSight database. If the application is showing incorrect device details (System Name, Contact, Location) or if device group membership is incorrect (particularly the system-created device groups), use this menu option to synchronize the device tree to the data in the database.	My Network Folder
<b>Remove From Group</b>	Removes the selected item from the group without deleting it from the database	Devices in User-Created Groups VLAN Port Templates
<b>Rename</b>	Highlights the selected item name to allow typing a new name.	Device User-Created Group VLAN Port Template
<b>Save Active to Startup</b>	Saves changes that you've made to a router's active configuration to its startup configuration. This assures that the currently active configuration will be reloaded when the router is rebooted.	Device Device Group All Devices Folder
<b>SSH</b>	Launches the Secure Shell (SSH) server and, after entering an appropriate username, opens a shell window, which provides the means to communicate with networking devices using a secure command-line based mechanism.	Device
<b>Start Compass Search</b>	Opens the <a href="#">Compass tab</a> and starts the Auto Search.	Device
<b>Syslog Receiver Configuration</b>	Launches the <a href="#">Syslog Receiver Configuration</a> window where you can set the IP addresses for those Syslog Receivers on your network devices so that the devices in your network will know where to send Syslog messages.	Device, Device Group

Menu Selection	Definition	Available From
<b>Trap Receiver Configuration</b>	Launches the <a href="#">Trap Receiver Configuration</a> window where you can view and define the information needed to receive SNMPv1/v2 and SNMPv3 trap information from the devices on your network.	Device, Device Group
<b>Telnet</b>	Launches a telnet session to the selected device's Local Management.	Device
<b>View Current Alarms</b>	Displays current alarm information for the device and lets you clear selected or all alarms, as well as view an alarm history for the device.	Device
<b>View Device Details</b>	Provides access to various Management Center and Console FlexView reports.	Device
<b>WebView</b>	Launches WebView Web Based Management, which lets you configure and manage certain Extreme Networks and Enterasys devices via a web browser from any location in the network.	Device (only available with certain Extreme Networks and Enterasys devices)

## Related Information

For information on related windows:

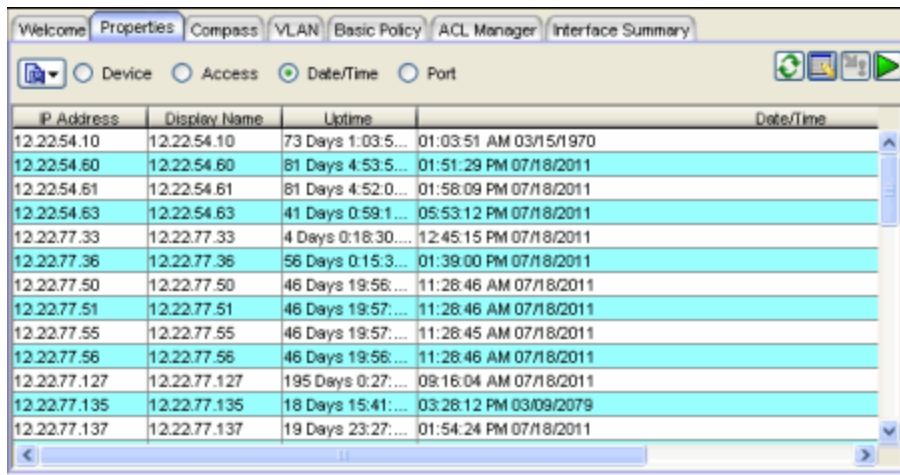
- [Main Window](#)
- [Menu Bar](#)
- [Tool Bar](#)
- [Right Panel](#)
- [Status Bar](#)

## Main Window Right Panel

---

The object selected in the left panel determines what appears in the right panel. When an object in the My Network branch of the hierarchy is selected, the following default tabs are available in the right panel:

- [Properties](#) - This tab is presents a table of in-depth information about the devices or device groups selected in the left panel. Four radio buttons let you select between device properties, access properties, date/time, or port properties. Console's Table Editor feature lets you modify and set writable properties in selected devices.
- [Compass](#) - Compass is a search tool that provides information about the status, configuration, and activities at the ingress points of your network. The devices or device group(s) selected in the left panel determine the scope of the search.
- [VLAN](#) - This tab provides views of VLAN device and port settings and enables you to analyze, modify and enforce VLAN settings using VLAN models.
- [Basic Policy](#) - The Basic Policy Tab displays the default policy role configured for each port and lets you change the role, if desired.
- [ACL Manager](#) - ACL Manager provides the tools that let you efficiently manage the Access Control Lists (ACLs) on your Extreme Networks routers.
- [Interface Summary](#) - This tab presents a default [FlexView](#) that shows basic interface information (speed, IP Address, type of interface) for the current left panel selection(s) and allows you to filter the table information based on the interface type.

*Sample Right Panel*

The screenshot shows a network management interface with a table of IP addresses. The table has four columns: IP Address, Display Name, Uptime, and Date/Time. The rows are sorted by uptime, with the longest uptime at the top. The interface includes a menu bar with options like Welcome, Properties, Compass, VLAN, Basic Policy, ACL Manager, and Interface Summary. Below the menu bar, there are radio buttons for Device, Access, Date/Time (selected), and Port. There are also several icons on the right side of the interface.

IP Address	Display Name	Uptime	Date/Time
12.22.54.10	12.22.54.10	73 Days 1:03:5...	01:03:51 AM 03/15/1970
12.22.54.60	12.22.54.60	81 Days 4:53:5...	01:51:29 PM 07/18/2011
12.22.54.61	12.22.54.61	81 Days 4:52:0...	01:58:09 PM 07/18/2011
12.22.54.63	12.22.54.63	41 Days 0:59:1...	05:53:12 PM 07/18/2011
12.22.77.33	12.22.77.33	4 Days 0:18:30...	12:45:15 PM 07/18/2011
12.22.77.36	12.22.77.36	56 Days 0:15:3...	01:39:00 PM 07/18/2011
12.22.77.50	12.22.77.50	46 Days 19:56:...	11:28:46 AM 07/18/2011
12.22.77.51	12.22.77.51	46 Days 19:57:...	11:28:46 AM 07/18/2011
12.22.77.55	12.22.77.55	46 Days 19:57:...	11:28:45 AM 07/18/2011
12.22.77.56	12.22.77.56	46 Days 19:56:...	11:28:46 AM 07/18/2011
12.22.77.127	12.22.77.127	195 Days 0:27:...	09:16:04 AM 07/18/2011
12.22.77.135	12.22.77.135	18 Days 15:41:...	03:28:12 PM 03/09/2079
12.22.77.137	12.22.77.137	19 Days 23:27:...	01:54:24 PM 07/18/2011

**Related Information**

For information on related windows:

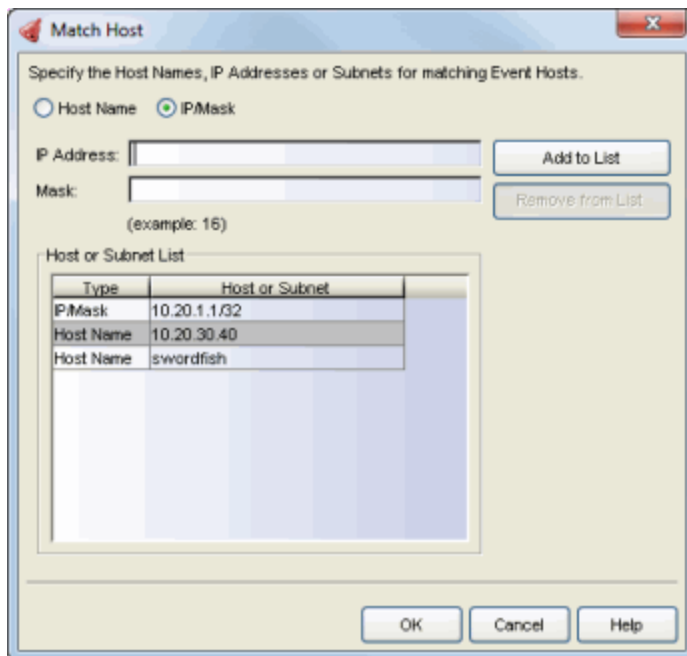
- [Main Window](#)
- [Menu Bar](#)
- [Tool Bar](#)
- [Left Panel](#)
- [Status Bar](#)

## Match Host Window

---

The Match Host window lets you manage a list of host names, IP addresses, or subnet addresses that will be used as "Match on Host or IP/Subnet" attributes in the [Edit Custom Alarm Criteria window](#). The host or IP/subnet list will be used as criteria to determine whether an alarm will be triggered.

Select the Host Name or IP/Mask radio button depending on what kind of attribute you want to add to the list. Enter the host name or IP address of a specific device, or the IP address and mask for a specific subnet. Click **Add to List** and then click **OK** to close the window. The list will be displayed in the Edit Custom Alarm Criteria window.



---

### Related Information

For information on related windows:

- [Edit Custom Alarm Criteria Window](#)
- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Custom Alarm Criteria](#)

## Match Phrase List Window

---

The Match Phrase List window lets you manage text strings (phrases) and regular expressions that will be used as "Match on Information Text" attributes in the [Edit Custom Alarm Criteria window](#). The text strings will be used to match against text in the Information column of the event or trap to determine whether an alarm will be triggered.

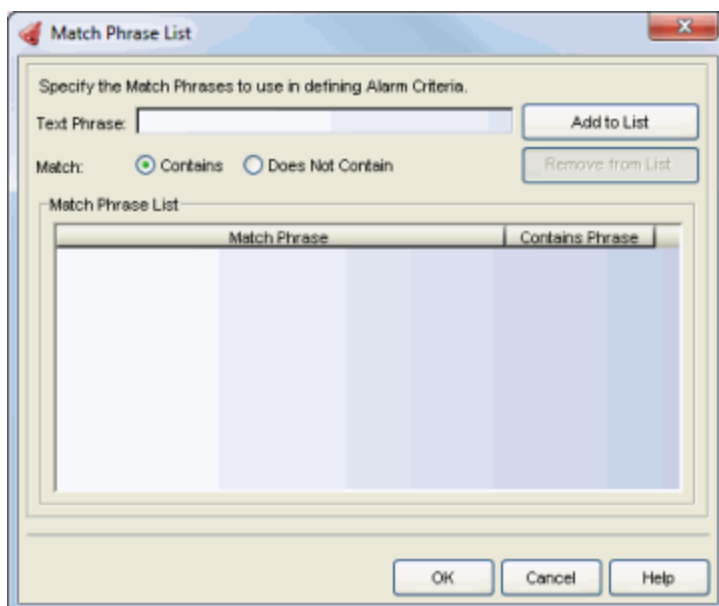
In the Text Phrase field, enter the text string that comprises the phrase or regular expression to be matched. Regular expressions let you create search arguments that provide a powerful tool for matching text strings. For example, the expression **Up|Down** will match either *Up* or *Down*. A summary of supported expressions can be found at:

<http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html>.

Select the appropriate Match option:

- **Contains** - A match occurs when the informational message contains the Text Phrase.
- **Does Not Contain** - A match occurs when the informational message does not contain the Text Phrase.

Click **Add to List** and then click **OK** to close the window. The list will be displayed in the Edit Custom Alarm Criteria window.



## Related Information

For information on related windows:

- [Edit Custom Alarm Criteria Window](#)
- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Custom Alarm Criteria](#)



## Menus

---

NetSight Console menus provide access to tools and functions that help you manage your network. Console menus are available in several forms, designed for your convenience when accessed in a given situation. Many of the options available from menus are also available as buttons on one or more toolbars. Icons associated with these menu options indicate when the same option is available from a toolbar. Specific menu options are dynamically enabled and disabled depending on which window, object, and tab is selected.

Here are the types of menus that you'll find in Console:

- [Main Window Menu Bar](#)
- [Left Panel Right Click Popup Menus](#)
- Table Tools (Right Click Popup Menus)
- [Drop-down Menu Buttons](#)

### Main Window Menu Bar

The main window menu bar provides access to functions that serve the overall operation of Console. The main window [Toolbar](#) and left panel [Right-click](#) menus provide many of the same options available from the menu bar.

The following menus are available on the menu bar:

*Click menus for more information.*



#### *File Menu*

##### **ACL Manager Database > Properties**

Opens the ACL Manager [Database Properties window](#) where you can view information about the database contents.

##### **ACL Manager Database > Initialize all ACL Manager components**

This menu option provides a way for you to initialize only the ACL Manager components in the NetSight Database. Using this operation instead of the Restore Initial Database function (accessed in the Server Information window) allows you to initialize your ACL Manager components while

---

retaining your other NetSight data elements in the database. It is recommended that you make a backup of your NetSight Database prior to performing the initialize operation by using the Backup Database window accessed from the Server Information window.

**Device List > Export**

Saves the content of the currently selected Device Group as a text file listing all of the devices in a format that can be imported by other NetSight applications.

**Device List > Import Devices**

Opens a file browser where you select a previously exported device list to be imported into the currently selected Device Group.

**Exit**

Exits NetSight Console.

*Edit Menu***Cut, Copy, and Paste**

These selections let you move, copy and paste devices and other objects in the left panel.

**Add Device**

Opens the Add Device window where you can define the IP address and community name for a device being added to the selected group.

**Add Device Group**

Opens the Add Device Group window where you can enter a name for a new group and add it to the left tree panel.

**Rename Device Group**

Highlights the selected group name to allow typing a new name.

**Delete Device(s)**

Removes the selected device from the NetSight database.

**Delete Device Group**

Removes the selected Group from the left panel.

**Remove From Device Group**

Removes the selected item from the group without deleting it from the database.

## Tools Menu



### Authorization/Device Access

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in NetSight applications.



### Server Information

Opens the Server Information window where you can view and configure certain NetSight Server functions, including management of client connections, locks, and licenses.



### Discover

Opens the Discover tool where you can discover devices on your network and populate the NetSight database.

### NetFlow Sensor Configuration

Opens the [Flow Sensor Configuration window](#) where you can enable or disable NetFlow on your network devices that support it.

### MIB Tools

Opens the MIB Tools that allows you to navigate the supported MIBs, examine MIB objects and perform SNMP sets to change their value.

### FlexView

These selections let you add and remove tabs for FlexViews in the right panel and Find, Filter, Sort, Print and Export the information in FlexViews.

- **Add FlexView Tab** - Adds a new FlexView tab in the right panel. Once the tab is added you can select a specific FlexView and its title will appear on the tab.
- **Remove FlexView Tab** - Deletes the currently selected FlexView tab from the right panel.
- **Find in FlexView** - Opens the Find toolbar at the top of the table in the right panel.
- **Filter FlexView** - Opens the Filter toolbar at the top of the table in the right panel.
- **Sort FlexView** - Opens the Sort toolbar at the top of the table in the right panel.
- **Export FlexView** - Exports the currently selected FlexView. When a Pie Chart or Bar Graph is displayed, the information is exported to a

GIF formatted image file. When a table is displayed, the table information is exported to an HTML file or Delimited Text file.

- **Print FlexView** - Prints the currently selected FlexView tab.

### Alarm/Event

**Alarms Manager** - The Alarms Manager window is where you can configure alarms when certain trap/event conditions occur on your network.

**Event View Manager** - 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.

### TFTP

**Firmware Image Download** - Opens the [Firmware Image Download window](#) which enables you to download a firmware image file to a device.

**Configuration Upload/Download** - Opens the [Configuration Upload/Download window](#) where you can upload configuration files from devices to save them elsewhere as backups, or download configuration files to devices. Using these functions, you can copy configuration files from one device to another.

### Options

Opens the **NetSight Console Options** window where you can set suite-wide and Console options.

### Wireless Manager

Launches the NetSight Wireless Manager, a tool that enables you to configure and manage multiple ExtremeWireless wireless controllers and their associated wireless APs.

### Policy Control Console

Launches Policy Control Console, a separately licensed tool that allows IT to delegate control of network usage to less technical personnel.

### RoamAbout Wireless Manager

Launches the RoamAbout Wireless Manager, a tool that provides network management for Wireless RoamAbout Access Points and RoamAbout R2 devices.

### *Applications Menu*

Lets you launch other installed NetSight applications from Console. You can also customize the Applications menu to launch your own applications. For more information, see [How to Add Applications to the Applications Menu](#).

## *Help Menu*

### **Help Topics (Contents)**

Opens the help browser to the Help System Welcome topic where you can access all of Console's online help topics.

### **NetSight Tips and Tutorials**

Opens your system's Web browser and takes you to the NetSight Tips and Tutorials where you can access Flash tutorials on the NetSight suite of products.

### **Release Notes**

Opens the help browser to the Release Notes that were effective when this version was installed. For more current information, visit the Network Management Suite (NMS) Documentation web page: <https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx> and open/download the latest version of the NetSight Console Release Notes.

### **Support Center (Help Center)**

Opens your system's Web browser and takes you to the Extreme Networks Support Web page.

### **Check for Updates**

Allows you to update Console with the latest software patches. Refer to the Suite-Wide Tools Web Update Help topics for more information.

### **Getting Started**

Opens the Getting Started Help information to introduce first-time users to the features in NetSight Console.

### **About This Window**

Displays help for the content currently displayed in the Main window.

### **About NetSight Console**

Displays the revision and copyright notice information for the currently installed version of NetSight Console.

---

## **Related Information**

For information on related windows:

- [Main Window](#)
- [Left Panel - Right-click Menus](#)

- [Toolbar](#)
- [Status Bar](#)

## MIB Tools Window

---

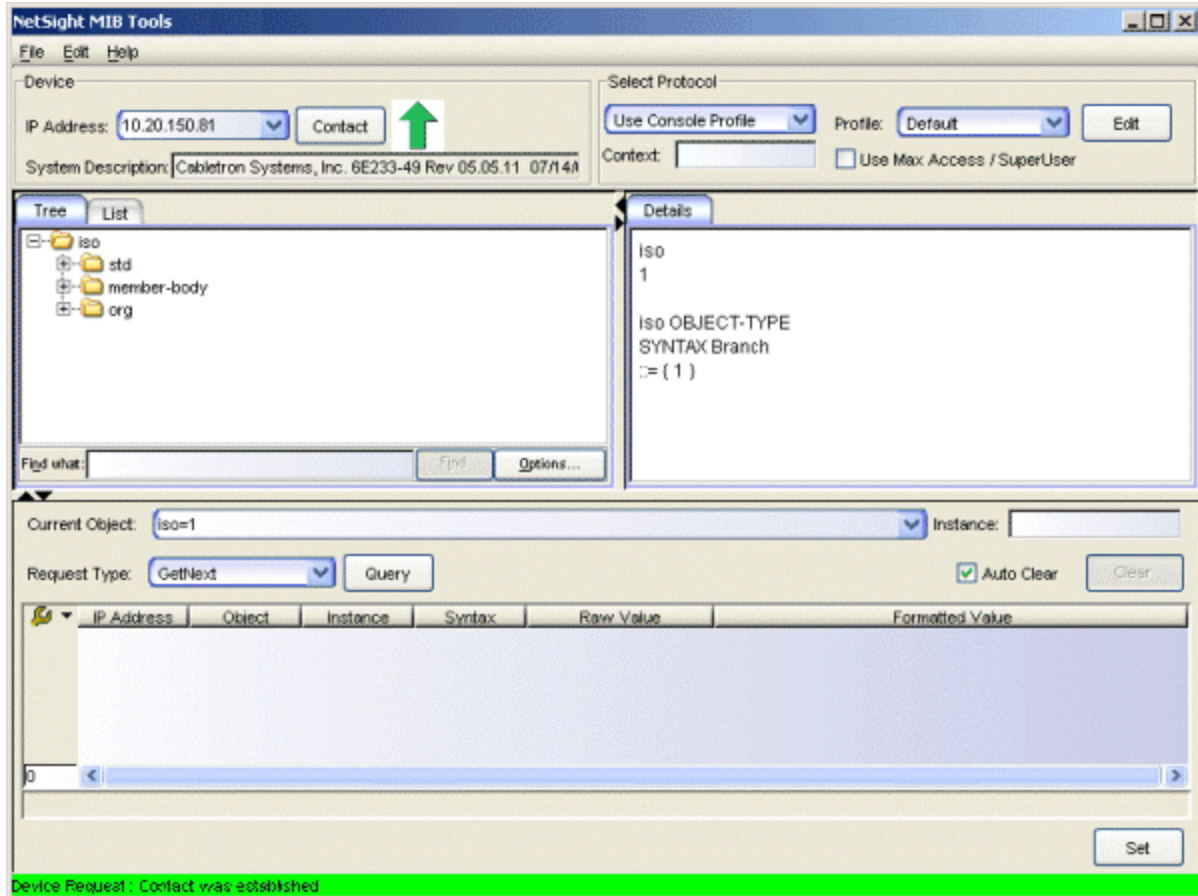
MIB Tools lets you examine the MIBs supported by an active device on your network and change the value of a writable MIB object and add instances of certain objects. Use the MIB Tools window to contact a device, view its supported MIBs, query the device for MIB values, and set a new value for a MIB object at the device. For more information on MIBs, see [MIB Tools Overview](#).

The MIB Tools window is divided into several sections and tabs:

- [Device](#) - Use this area to specify the device you wish to contact with MIB requests.
- [Select Protocol](#) - Use this area to specify the SNMP protocol you wish to use to contact the device.
- [Tree Tab](#) - Displays the MIB database in a tree format.
- [List Tab](#) - Displays the MIB database in a list format.
- [Details Tab](#) - Provides detailed information about the MIB branch or leaf object selected in the Tree or List tab.
- [Current Object](#) - Use this area to perform a Query operation. A Query finds the current value set at the selected device for a specified MIB object.
- [Results Table](#) - Provides the results of device queries for MIB values, and lets you change the value of a writable MIB object.

The Menu Bar at the top of the window lets you access the [MIB Tools Options window](#) (**Edit > Options**) and Help. The Status Bar at the bottom of the window displays error and status information.

To access MIB Tools, select **Tools > MIB Tools** from the Console menu bar, or right-click a device in the Console left panel and select MIB Tools from the menu.



## Related Information

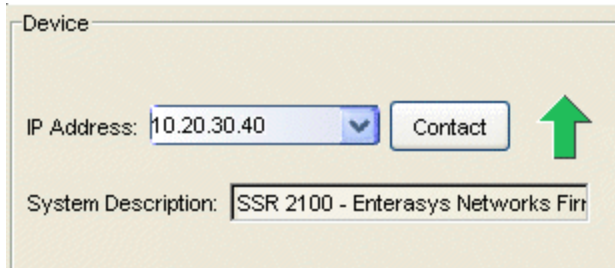
For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools Device

Use the Device area located at the top left of the [MIB Tools window](#) to specify the device you wish to contact with MIB requests. If you launched MIB Tools from a device selected in the Console's left panel, MIB Tools automatically attempts to contact the selected device.





### IP Address

Enter an IP address or use the drop-down list to select a previously contacted device. The Device tab in the MIB Tools Options window lets you set the number of IP addresses that will be saved between MIB Tools sessions, with a maximum of 9. The default number is 5.

### Contact/Stop Button

After entering an IP address and the appropriate protocol access information (in the [Select Protocol area](#)), click the **Contact** button to initiate contact with the device. The button changes to **Stop** while a contact request is being made.

### Contact Icon

The color-coded icon indicates the current state of communication between MIB Tools and the device. You can also click the icon to initiate contact with a device. This icon displays the results only for the device contact request.

- **Up Arrow/Green** -- the device has responded to the MIB Tools request. This icon will be displayed even if the device has responded with an error.
- **Hourglass/Beige** -- MIB Tools is attempting to contact the device.
- **?/Yellow** -- the contact status is unknown.
- **Down Arrow/Red** -- the device has not responded and the MIB Tools request has timed out.

### System Description

When a device is contacted, the system description is automatically displayed in this field. Use the tooltip to view the entire contents of the field. This is the same information that is returned from a query of the sysDescr OID.

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)

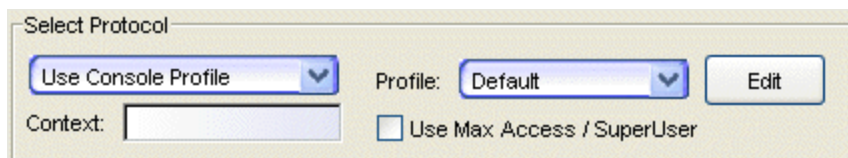
For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

---

## MIB Tools Select Protocol

Use the Select Protocol area located at the top right of the [MIB Tools window](#) to specify the SNMP protocol to use to contact the device.



The screenshot shows a dialog box titled "Select Protocol". It contains a dropdown menu with "Use Console Profile" selected, a "Profile:" dropdown with "Default" selected, and an "Edit" button. Below these is a "Context:" text input field and a checkbox labeled "Use Max Access / SuperUser" which is currently unchecked.

### Select Protocol

This drop down list lets you select the protocol and context for MIB queries/sets.

### Use SNMPv1/v2

Select SNMPv1 or SNMPv2 and enter a community name or use the drop-down list to select a community name. The permissions assigned to the community name you enter here will determine the level of access you have to the device's MIB information: Read Only, Read-Write, or Superuser. Be sure to use a community name with the appropriate level of access.

### Use SNMPv3 Credential

Select SNMPv3 and use the drop-down list to select a profile that will be used to contact a device. To create or edit a credential, click **Edit** to open the [Edit Credentials window](#). When SNMPv3 is selected, you can also specify a Context.

### Use Console Profile

Select this option to use a Console Profile and use the drop-down list to select a profile. To create or edit a profile, click **Edit** to open the Authorization Configuration/Device Access Window - Profiles/Credentials Tab. When SNMPv3 is selected, you can also specify a Context.

### Context

Some devices that support SNMPv3 are capable of restricting access to specific MIB objects based on a SNMP Context setting. When used, with SNMPv3 credentials, this entry provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted, but the context specified doesn't match one configured on the device, access is denied.

### Use Max Access/SuperUser

If you have selected Use Console Profile, you can select this checkbox to specify max access/superuser access for all requests.

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)

For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

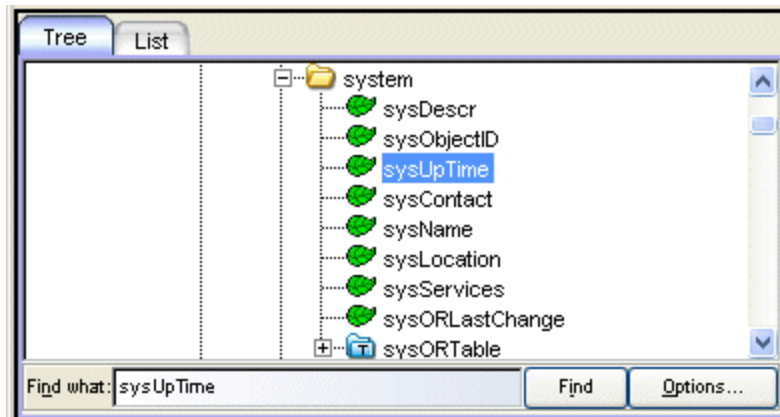
## MIB Tools Tree Tab

---

The left-panel Tree tab displays the MIB tree, a graphical directory of the MIB database. Like a file directory tree, the MIB Tree is represented by a series of collapsible and expandable folders, with the individual MIB Objects represented by leaves. Select a MIB branch or object by clicking on its corresponding folder or leaf icon; double-click to open a folder and display its contents. The currently selected branch or object is identified immediately below the Tree tab in the [Current Object field](#) by its text name and OID and is displayed in the [Table Editor](#) row of the [Results Table](#). For more information on how MIBs are organized, see [MIB Tools Overview](#).

You can search the MIB tree using the Find function.

### Sample MIB Tree



### Branch Folders

Each branch of the tree is indicated by a folder. The folder is marked with a minus sign (-) to denote that it has been expanded or with a plus sign (+), indicating that it can be expanded.

### Leaf Objects

Individual MIB objects are represented by leaves.

### Find what

Enter the MIB text name or OID you want to find.

### Find

This button starts the find operation and highlights (selects) the first matching entry. Click **Find** again to highlight the next matching entry.

### Options Button

This button opens the Options window where you can specify different attributes for the Find operation. For more information on Find options, see the Find Toolbar Options Help topic.

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)

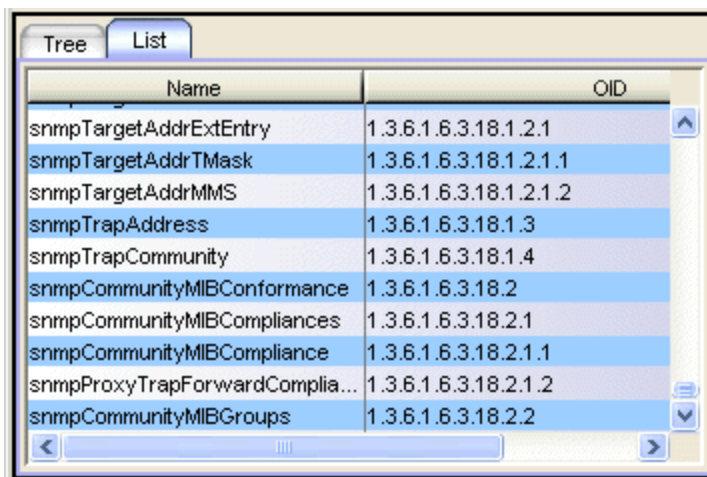
For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools List Tab

The left-panel List tab displays the MIB database in a list format. If you select an object in the List tab and return to the Tree tab, the selected object will be highlighted in the tree.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.



The screenshot shows a window with two tabs: 'Tree' and 'List'. The 'List' tab is active, displaying a table with two columns: 'Name' and 'OID'. The table contains the following entries:

Name	OID
snmpTargetAddrExtEntry	1.3.6.1.6.3.18.1.2.1
snmpTargetAddrTMask	1.3.6.1.6.3.18.1.2.1.1
snmpTargetAddrMMS	1.3.6.1.6.3.18.1.2.1.2
snmpTrapAddress	1.3.6.1.6.3.18.1.3
snmpTrapCommunity	1.3.6.1.6.3.18.1.4
snmpCommunityMIBConformance	1.3.6.1.6.3.18.2
snmpCommunityMIBCompliances	1.3.6.1.6.3.18.2.1
snmpCommunityMIBCompliance	1.3.6.1.6.3.18.2.1.1
snmpProxyTrapForwardComplia...	1.3.6.1.6.3.18.2.1.2
snmpCommunityMIBGroups	1.3.6.1.6.3.18.2.2

### Name

The text name for each MIB object.

### OID

The OID (Object Identifier) for each MIB object.

## Related Information

For information on related windows:

- [MIB Tools Window](#)

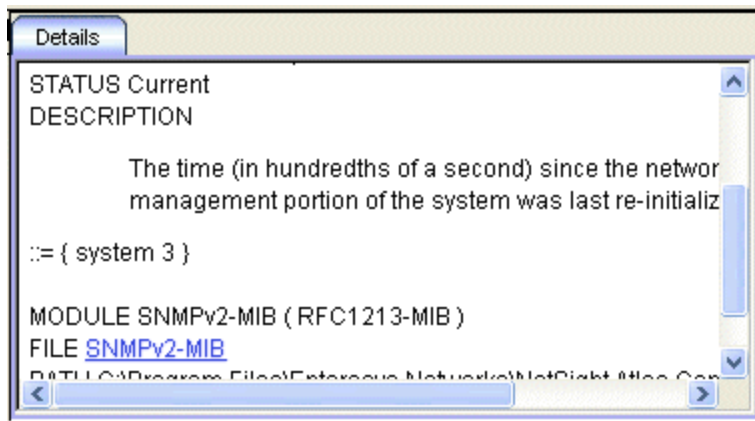
For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools Details Tab

The right-panel Details tab displays information about the MIB branch or leaf object selected in the [Tree tab](#) or [List tab](#). The currently selected branch or object is identified immediately below the Tree tab in the Current Object field by its text name and OID (Object Identifier).

The Details tab fields vary depending on the selected MIB object; some common fields are defined below.



### Full Path

The full path to the MIB object as a text string.

### OID

The full path to the MIB object as a numeric OID (Object Identifier).

### Object Type

The defined name of the object.

### Syntax

The way data represented by this object is structured in the device MIB: Integer, Octet String, Object Identifier, Null, Sequence, Sequence of, IpAddress, NetworkAddress, Counter, Gauge, TimeTicks, Opaque, or some other user-defined data type.

### Textual Convention

A refinement of a data type.

### Display-Hint

A hint regarding how a value corresponding to a textual convention might be displayed.

**Max Access**

The level of maximum management access available for this specific object: Read Only (instances of the object may be read, but not set), Read/Write (instances of the object may be read or set), Write-Only (instances of the object may be set but not read), or No Access (instances of the object may not be read or set). Note that this does not designate the level of access provided by the community name you used to contact the device, but the maximum level of access available for the object by definition.

**Status**

Indicates the status of the textual convention: Current, Deprecated, or Obsolete.

**Description**

A brief textual description of the management information conveyed by this object.

**Module**

The module that this MIB object belongs to.

**File**

The MIB module file name. Clicking the MIB filename opens a window showing the complete text of the MIB together with search features to help in locating specific information.

**Path**

The path to where the MIB file is located.

---

**Related Information**

For information on related windows:

- [MIB Tools Window](#)

For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools Current Object

Use this area in the MIB Tools window to perform a Query operation on the selected device. A Query finds the current value set on the device for the MIB object specified in the Current Object field. The results of a query operation are displayed in the [Results Table](#) at the bottom of the window.

The screenshot shows a user interface for the MIB Tools window. It features a 'Current Object' field with a text input containing 'sysUpTime=1.3.6.1.2.1.1.3' and a dropdown arrow on the right. To the right of this field is an 'Instance' field with an empty text input. Below the 'Current Object' field is a 'Request Type' dropdown menu set to 'Get', a 'Query' button, a checked 'Auto Clear' checkbox, and a 'Clear' button.

### Current Object

To perform a Query, enter the folder or object's name or OID. You can also select a MIB object leaf or folder in the Tree or List tab, and the name and OID will be automatically entered in the Current Object field. Clicking the down arrow at the right end of the field shows a drop-down list of recent selections. The number of selections depends on the setting on the [Object](#) tab in the MIB Tools Options window. The default is 5 objects with a maximum of 9.

### Instance

For objects with multiple instances, enter the instance number to be used for a Get request. For example, if you are querying a switch's interface table, there would be multiple instances (values) returned for each leaf object in the table (one for each port), and each instance would have a unique instance value appended to the object's OID.

### Request Type

Use the drop-down list to select the type of request to send to the selected device:

- **GetNext** -- requests all the instances of the MIB object specified in the Current Object field.
- **Get** -- requests the first instance of the MIB object specified in the Current Object field.
- **Single GetNext** -- requests the next single instance of the MIB object specified in the Current Object field.

### Query/Stop

Starts the Query operation. Results are displayed in the Results table at the bottom of the MIB Tools window. The Status Bar at the bottom of the window will inform you about the progress of your query. The button



changes to **Stop** while a Query is being performed. If you stop the Query operation, the query will be canceled, but all values returned before the query was stopped will remain in the Results Table.

**Auto Clear**

When checked, the Results table is cleared whenever the **Query** button is clicked.

**Clear**

Removes all the entries from the Results table.

---

**Related Information**

For information on related windows:

- [MIB Tools Window](#)


For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools Results Table

---

The Results table at the bottom of the [MIB Tools window](#) contains all information returned by the selected device in response to a request (query) initiated on a MIB branch or leaf. The Table Editor at the bottom of the Results table lets you change the value of a writable MIB object.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools 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). For more information, see the Table Tools Help topic.

Row Count	IP Address	Object	Instance	Syntax	Raw Value	Formatted Value
1	10.20.30.7	ifAdminStatus	1	integer	1	up
2	10.20.30.7	ifAdminStatus	2	integer	1	up
3	10.20.30.7	ifAdminStatus	3	integer	1	up
4	10.20.30.7	ifAdminStatus	4	integer	1	up
22	10.20.30.7	ifAdminStatus	1	integer	1	up

Object Query: Successfully completed GetNext request

### Row Count Column

Each row in the table has a unique line number. This is useful for restoring the rows to their original order after you have sorted the table. The total number of rows is displayed at the bottom of the column.

### IP Address

The IP address of the queried device.

### Object

The name of the MIB object. For writable MIB objects, you can change this value using the [Table Editor](#).

### Instance

The specific occurrence of the object to which the returned value pertains. Some objects may have more than one occurrence, or instance, on the device. For example, a *sysContact* query returns a single value -- the designated contact person for system information or service. An *ifIndex* query will return a value for each interface index discovered on the selected device. An instance value of 0 indicates that the selected object can have only a single instance; an instance value greater than zero indicates that the object is part of a table, and may have multiple instances. For writable MIB objects, you can change this value using the [Table Editor](#).

### Syntax

The structure of the data in the returned value. A MIB Object may have one of the following types:

- Integer -- A data type taking a cardinal number as its value. The number may have a symbolic name associated with it. For example, an interface's administrative status, *ifAdminStatus*, returns as an integer representing one of three administrative states: up(1), down(2), or testing(3).
- Unsigned Integer

- Counter --A data type representing a non-negative integer, which increments until it reaches a maximum value (not to exceed  $2^{32}-1$ ), then it returns to zero. This data type is frequently used to measure statistical values, such as bytes processed by a device since start-up.
- Counter 64 -- A data type used only when a Counter would return to zero in less than one hour.
- Gauge --A data type representing a non-negative integer, which may increase or decrease, but latches at a maximum value (not to exceed  $2^{32}-1$ ). This would be used to measure both current and peak network traffic rate, for example.
- Time Ticks -- A data type representing a non-negative integer, which counts the time in hundredths of a second (not to exceed  $2^{32}-1$ ) since some epoch (e.g., time since device power-up).
- Bits
- Octet String -- A data type taking zero or more octets as its value. Each byte in the octet string can have a value from 0 to 255. For example, a device name would be encoded in an octet string.
- Display String
- OID -- A data type referring to an authoritatively named object in the MIB Tree. For example, *sysObjectID* returns each vendor's authoritative identification of their manageable devices, as recorded in their branch of the Internet MIB (internet > private > enterprises).
- IP address -- A data type representing an IP address .
- MAC Address -- A data type representing a MAC address.
- Opaque -- A data type representing an arbitrary encoding.
- Null -- A data type that can be used to represent a value that can be safely ignored.

For writable MIB objects, you can change this value using the [Table Editor](#).

### Raw Value

This is the value returned by the device and displayed exactly as it is. For writable MIB objects, you can change this value using the [Table Editor](#).

### Formatted Value

This is the value returned by the device and displayed in a format that is easier to understand. If no formatting is appropriate, the value will be the same as the raw value. For writable MIB objects, you can change this value using the [Table Editor](#).

## Table Editor

Use the Table Editor at the bottom of the Results table to change the Object, Instance, Syntax, Raw Value, and/or Formatted Value of a writable MIB object. Select the desired row in the Results table. In the Table Editor, change the desired values. Click the **Set** button. The Status Bar will display the results of the Set. If the Set was successful, click **Query** to refresh and update the Results table with the new values. For more information on using the Table Editor, see [Setting MIB Objects](#).

---

**CAUTION:** Setting certain MIB objects can disable devices and cause interruptions to network operation. Do not set MIB values unless you are sure of the outcome.

---

## Auto Clear

When checked, the table is cleared whenever the **Query** button is clicked.

## Clear

Removes all the entries from the Results table.

## Set/Stop

Sets the new values entered in the [Table Editor](#). The button changes to **Stop** when a Set request is issued.

## Find in MIB Tree

Right-click in the Results table and select the Find in MIB Tree menu option. The object currently selected in the Results Table is highlighted in the [Tree Tab](#) or [List Tab](#).

---

## Related Information

For information on related windows:

- [MIB Tools Window](#)

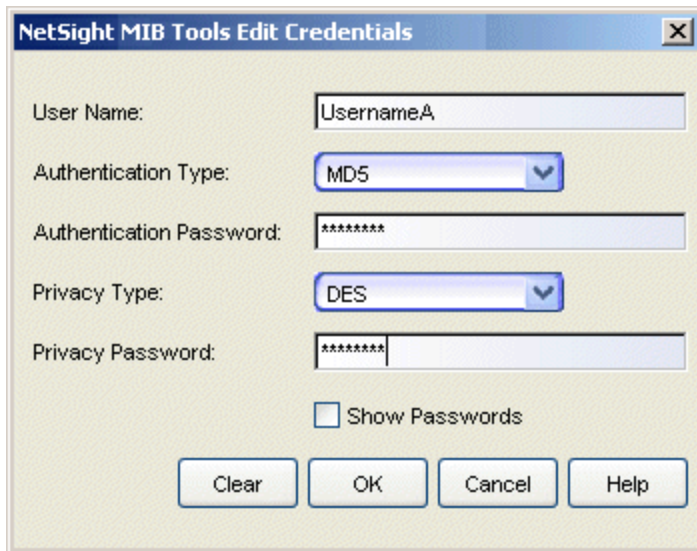
For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

## MIB Tools Edit Credentials Window

---

The Edit Credentials window lets you create or edit credentials for an SNMPv3 device selected in the [MIB Tools](#) window. To access the window, select the Use SNMPv3 Credential option in the Select Protocol area, and click the **Edit** button.



The screenshot shows a dialog box titled "NetSight MIB Tools Edit Credentials". It contains the following fields and controls:

- User Name:** A text input field containing "UsernameA".
- Authentication Type:** A dropdown menu with "MD5" selected.
- Authentication Password:** A text input field containing "\*\*\*\*\*".
- Privacy Type:** A dropdown menu with "DES" selected.
- Privacy Password:** A text input field containing "\*\*\*\*\*".
- Show Passwords:** An unchecked checkbox.
- Buttons:** Four buttons at the bottom: "Clear", "OK", "Cancel", and "Help".

### User Name

Enter the User Name for the credentials.

### Authentication Type

If the credential includes authentication, specify the authentication protocol to be used: MD5 or SHA1.

### Authentication Password

Enter the user's authentication password.

### Privacy Type

If the credential includes privacy, specify the privacy protocol to be used: DES (Data Encryption Standard).

### Privacy Password

Enter the user's privacy password.

### Show Passwords

When checked the Authentication Password and Privacy Password appear as text.

## Related Information

For information on related windows:

- [MIB Tools Select Protocol](#)

## MIB Tools Options Window

---

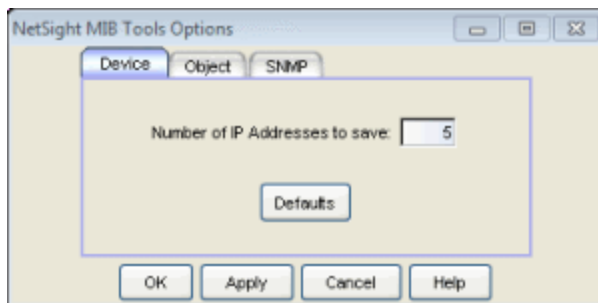
The Options window allows you to set options for MIB Tools functions. The window displays three tabs for the different options. To access the Options window, select **Edit > Options** from the [MIB Tools window](#) menu bar.

Information on the following tabs:

- [Device](#)
- [Object](#)
- [SNMP](#)

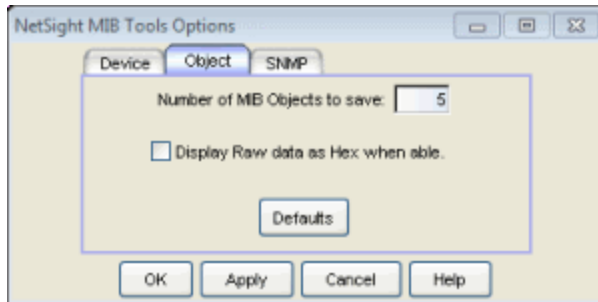
### Device Tab

This option lets you set the number of IP addresses that will be saved between MIB Tools sessions, with a maximum of 9. These IP addresses are displayed in the IP Address field drop-down list in the MIB Tools window [Device](#) area. As you contact devices, the IP address for each device is added to the list.



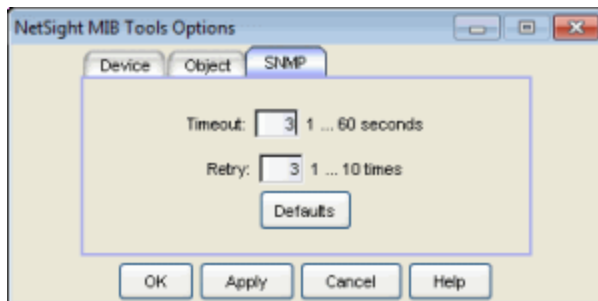
### Object Tab

This option determines the number of recent selections that will appear in the drop-down list for [Current Object](#) field, with a maximum of 9. Set the option if you want to display the raw value displayed in the Results table as Hex when possible.



## SNMP Tab

These options let you set the SNMP Timeout which is the interval in seconds between attempts to contact a device, and the SNMP Retry which is the number of attempts to make before abandoning attempts to contact a device.



## Related Information

For information on related tasks:

- [How to Use MIB Tools](#)
- [MIB Tools Overview](#)

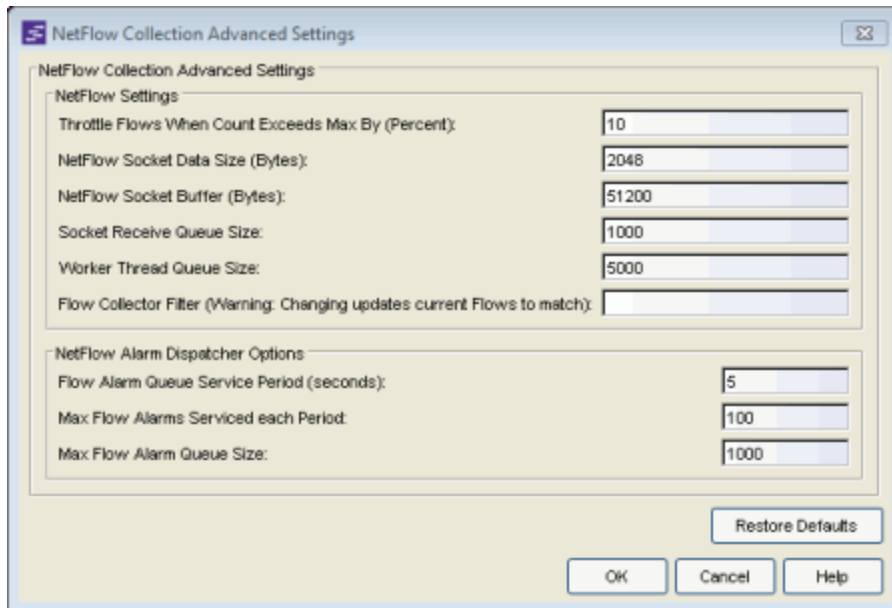
For information on related windows:

- [MIB Tools Window](#)



## NetFlow Advanced Settings Window

Use this window to configure advanced settings for the NetFlow flow collection and to limit resources used by NetSight Flow Alarm handling. You can access the window from the [NetFlow Collection view](#) in the Console options.



### NetFlow Settings

#### Throttle Flows When Count Exceeds Max By (Percent)

Flow collection will be throttled when the [Maximum Flows to Maintain in Memory](#) is exceeded by the percentage entered here.

#### NetFlow Socket Data Size

The socket data size in bytes. Typically, this setting should not be changed.

#### NetFlow Socket Buffer

The buffer size (in bytes) that will be set aside by the NetSight server for buffering incoming flows.

#### Socket Receive Queue Size

Network packets are retrieved from a datagram socket and put into a fixed-size queue for decoding into flow records. The queue can overflow if the receive rate exceeds the decoding rate. This option allows you to configure the queue size (number of network packets).

### **Worker Thread Queue Size**

Decoded flow records are put into one of several fixed-size queues for processing. These queues can overflow if the decoding rate exceeds the processing rate. This option allows you to configure the queue size (number of flow records).

### **Flow Collector Filter**

Use this field to filter all incoming flows as they are processed by the flow collector. Flows not matching the filter are discarded and not maintained in memory on the server. If you add a filter here, the current flows stored in the cache will be trimmed to only matching flows. This is useful if flow collection is to be used to look for specific results, and unrelated flows do not need to be processed. An example of this might be to only process flows pertaining to a particular subnet.

### **NetFlow Alarm Dispatcher Options**

When a flow matches an alarm definition, the match is moved into the Flow Alarm queue for processing by the NetFlow Alarm dispatcher, which gathers additional data and then generates the alarm. A specified number of matched flows are taken from the queue and processed once each service period, according to the option values specified here.

#### **Flow Alarm Queue Service Period**

This controls how often the queue is checked for matched flows to process. The dispatcher runs once every service period. So by default, the dispatcher processes matches every 5 seconds.

#### **Max Flow Alarms Serviced each Period**

The maximum number of matched flows pulled from the queue for processing each service period. By default, the dispatcher processes 100 matches every service period.

#### **Max Flow Alarm Queue Size**

The maximum number of matched flows that can be queued. By default, the dispatcher drops matched flows after 1000 matches are queued.

---

### **Related Information**

For information on related windows:

- [NetFlow Collection Options](#)

# OneView Collector Advanced Settings Window

Use this window to configure advanced settings for the Management Center data collector. You can access the window from the [OneView Collector view](#) in the Console options.

OneView Collector Advanced Settings

OneView Collector Advanced Settings

IP Address Format

Host Name Resolution:

Wireless Collection

Discover Engine Interval (seconds): 60

Poll Engine Interval (seconds): 10

Rediscover Interval (hours): 1

Client Cleanup Interval (hours): 168

Collection Client Limit: 2500

Time Between Collection Client Limit Events (hours): 24

Device Collection

Discover Engine Interval (seconds): 10

Poll Engine Interval (seconds): 10

Rediscover Interval (hours): 24

Interface Collection

Discover Engine Interval (seconds): 2

Poll Engine Interval (seconds): 1

Rediscover Interval (hours): 24

SNMP Settings

Max Outstanding SNMP Per Collector: 50

Monitor Collection

Monitor Mode Enabled:

Poll Engine Interval (seconds): 5

Time to Verify Monitor Targets Interval (hours): 24

Restore Defaults

OK Cancel Help

## Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for this feature only. (Host name resolution is enabled globally using the Suite Name Resolution option.)

Specify the following three options for your wireless controllers, devices, and interfaces that have collection enabled (called collection targets).

### **Discover Engine Interval**

This interval specifies the frequency that the data collector will perform discover operations on the collection targets. Discover operations are performed in blocks specified by the Max Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here. Valid values are 1-300 seconds.

### **Poll Engine Interval**

This interval specifies the frequency that the data collector will poll the collection targets. Polling is performed in blocks specified by the Max Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified here. Valid values are 1-300 seconds.

### **Rediscover Interval**

This interval specifies the frequency that the data collector will perform a rediscover operation on the collection targets. Valid values are 1-168 hours.

### **Client Cleanup Interval**

Wireless client statistics stored by the data collector are periodically cleaned up according to this interval. When the Collection Client Limit has been reached, clients that have been inactive longer than the time specified in the Time between Collection Client Limit Events will be aged out.

### **Collection Client Limit**

The maximum number of wireless clients that can have statistics stored per collection interval. Valid values are 1 to 5000.

### **Time between Collection Client Limit Events**

During a client cleanup, if a client has been inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

### **Max Outstanding SNMP per Collector**

The number of SNMP requests that a collector will make simultaneously. The data collector works with blocks of SNMP requests, starting a new block each time the outstanding block completes. Valid values are 1-500.

### **Monitor Mode Enabled**

Use this option to enable or disable Monitor mode statistic collection. If Monitor mode is disabled, the Monitor mode option will not be available when configuring device or interface statistics collection. All Monitor mode

statistic collection will be stopped and the monitor cache is cleared. For more information on the Monitor mode, see Enable Report Data Collection.

#### **Time to Verify Monitor Target Interval (hours)**

The interval between a Management Center check of all targets (devices and interfaces) set to Monitor mode statistic collection. The check generates a summary event in the Console event log (one for devices and one for interfaces) that shows the number of targets where corresponding threshold alarms are not configured. Those targets should have Monitor mode disabled, or appropriate threshold alarms should be configured, in order to reduce unnecessary statistic collection.

---

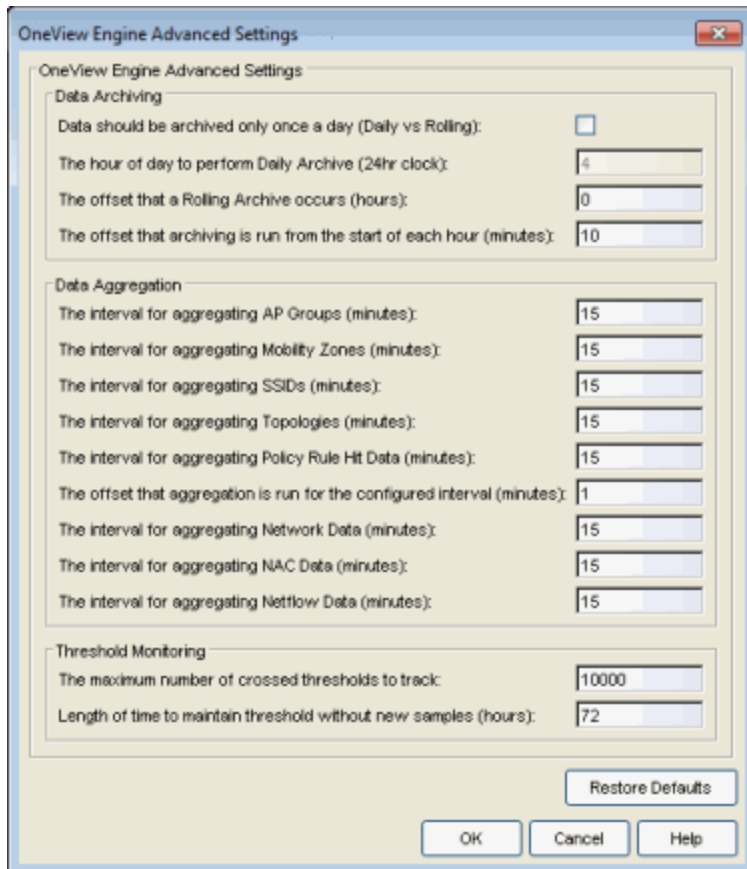
#### **Related Information**

For information on related windows:

- [OneView Collector Options](#)

# OneView Engine Advanced Settings Window

Use this window to configure data archiving, aggregation, and session limit settings for the OneView engine. You can access the window from the [OneView Engine view](#) in the Console options.



## Data Archiving

Use the data archiving settings to specify whether collection data should be archived on a daily basis or rolling basis (the default).

- **Daily Archive** - If you want all the collection data (including the raw data, and the hourly, daily, weekly, and monthly data) archived once a day at a certain time, select the checkbox and specify the hour of day to perform the daily archive.
- **Rolling Archive** - If you want the collection data to be archived on a rolling basis (archives are performed on an hourly, daily, weekly, or monthly basis as needed), specify the offset (in hours and minutes) that the rolling

archive will be performed, following the end of the data collection period. The offset allows for the time it takes for data to be collected and reported to the database. If the offset time is too short, then the archive may be performed before all the data is reported to the database. If you have a network scenario where there is a long latency in reporting data to the database, then you may need to increase the offset in order to make sure all the data is included in the archive.

### Data Aggregation

Use the data aggregation settings to specify how often collected data is aggregated into one statistic for AP Groups, Mobility Zones, SSIDs, Topologies, Policy Rule Hits, Network, NAC, and NetFlow. For example, the data collected for all the APs in an AP group will be aggregated into one AP Group statistic according to the specified interval. Intervals are based on the 0 minute of the hour, so if you have an interval of 15 minutes, the aggregation will be performed every 15 minutes starting from the top of the hour. The offset allows for the time it takes for data to be collected and reported to the database. If the offset is too short, then the aggregation may be performed before all the data is reported to the database. If you have a network scenario where there is a long latency in reporting data to the database, then you may need to increase the offset in order to make sure all the data is included in the aggregation.

### Threshold Monitoring

These settings apply to [threshold alarms](#):

- **Maximum number of crossed thresholds to track.** To prevent memory over-utilization, there is a maximum number of crossed threshold states that are maintained. The default maximum number is 10,000. If this number is exceeded, the oldest 10% are deleted and the associated alarm is cleared.
- **Length of time to maintain threshold without new samples.** Determines when a crossed threshold state will expire due to inactivity (no new samples received). The default length of time is 72 hours. If there are no samples received during this time period, the threshold state is deleted and the associated alarm is cleared.

---

### Related Information

For information on related windows:

- [OneView Engine Options](#)

## Ping Window

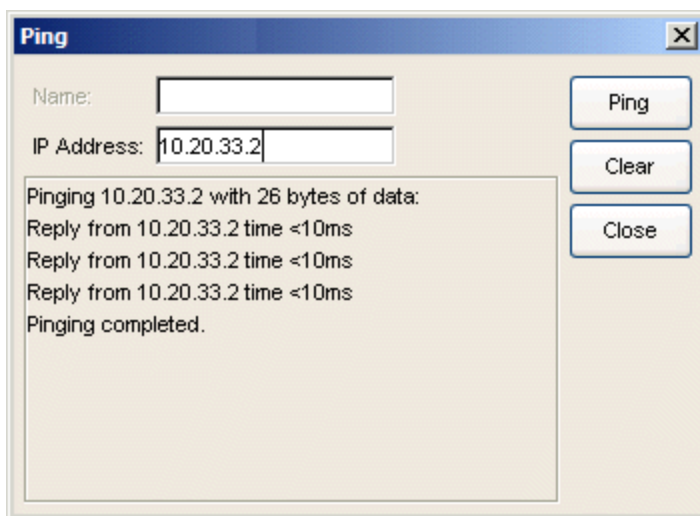
---

The Ping window provides the ability to ping an IP address to determine if the network element can be contacted. To access this window, open the [Compass tab](#) and select IP Address from the Search Type drop-down list. Then enter the IP address or host name for the network element in the "IP Address or Host Name" field, and click **Ping Address**. The Ping window opens, and the network element is automatically pinged. You can view the results of the ping in the log on this window. You can click **Clear** to enter another IP address or host name to ping, if you wish.

---

**NOTE:** On a Windows platform, ping will not work unless you are logged on and running Console as a user with Administrative privileges.

---



### Name

Host name of the network element you want to ping. You can enter this, or the IP address.

### IP Address

IP address of the network element you want to ping. You can enter this, or the host name.

### Ping Log

Displays the results of the ping.



### **Ping Button**

Attempts to contact the IP address or host name currently displayed. The system attempts three pings.

### **Clear Button**

Clears the currently displayed data.

---

## **Related Information**

For information on related tasks:

- [How to Use Compass](#)
- [Pinging](#)

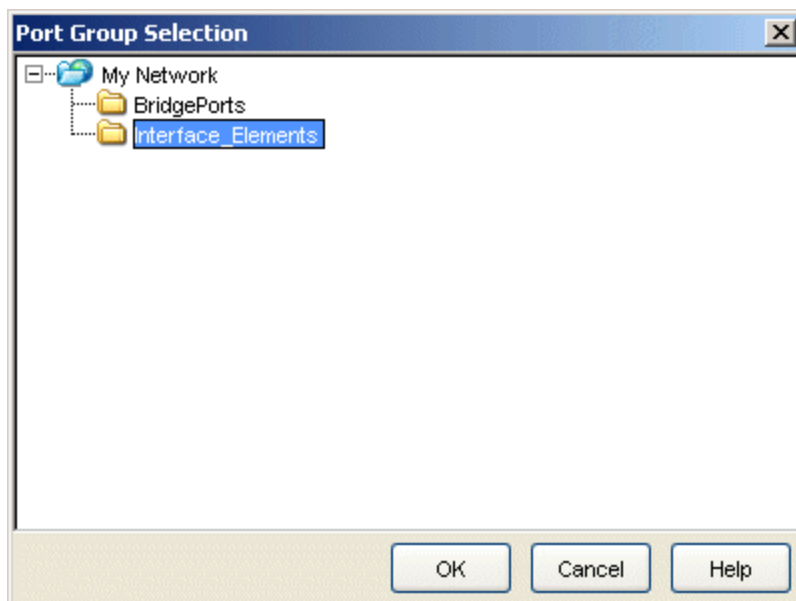
For information on related windows:

- [Compass Tab IP Address Search](#)

## Port Group Selection Window

---

The Port Group Selection window lets you add individual ports selected from a [FlexView](#) table to the **My Network** folder or to a user-created group in the left panel. When added to the tree, the ports are also added to the **All Port Elements** system-created group. Individual ports are used with FlexViews to query information specific to interfaces, bridge ports and other port types. Ports are added to the left panel by choosing **Add Port Elements to Group** from the right-click menu in a FlexView table.



---

### Related Information

For information on related windows:

- [Main Window](#)
- [Left Panel](#)
- [FlexView Tab](#)

For information on related tasks:

- [How to Add and Remove Port Elements](#)

## Port Monitor Window

---

The Port Monitor window lets you view a variety of detailed port information and statistics presented together in one place. To launch the Port Monitor, right-click on a port in any of the following NetSight views and select Port Tools > Port Monitor from the menu.

- Console Properties Tab (Ports View)
- Console Compass Tab (Results Tab)
- Console FlexViews Tabs (for example, the Interface Summary Tab)
- Console tree
- Console VLAN Basic Port and Advanced Port views
- ASM Activity Monitor tree
- NAC Manager End-Systems Tab
- Policy Manager device Details View tab and Ports tab

Use the **Options** button at the bottom of the window to open the Suite-Wide Options Port Monitor Options panel where you can customize what Port Monitor information will be displayed. Use the arrows on the right-hand side of the window to expand and collapse the different sections of information.

The port data is read from the device when the window is first opened, and then can be updated using the **Refresh** button. The exception to this is the Statistics data presented in the Port Information section that is polled from the device according to the poll interval specified in the Port Monitor Options panel. Use the **Export** button to export the Port Monitor data to an HTML file that you can then save, email, or print.

Sample Port Monitor Window



**Port Information**

This section provides detailed port information including port name, type, and status information along with port traffic statistics. The statistics are polled from the device and two poll cycles must be completed before information will be initially displayed. All other port information is read from the device when the window is first opened, and can be updated using the

**Refresh** button. Use the **Options** button at the bottom of the window to open the Port Monitor Options panel where you can specify polling options. You can also enable and disable the display of the port information statistics in the Options panel.

## VLAN

This section displays the VLAN settings for the port. For more information on the data presented, refer to the [VLAN Tab](#) or [VLAN Concepts](#) Help topics, or see the following links:

- [PVID](#)
- [Default Port Priority](#)
- [Ingress Filtering](#)
- [Acceptable Frame Types](#)
- [Current Egress](#)
- [Static Egress](#)
- [GVRP](#)

## Policy

This section displays the policy settings for the port. For more information on the data presented, refer to the [Basic Policy Tab](#), General Tab (Role), and General Tab (Rule) Help topics. You can enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

## Authentication

This section displays the authentication settings for the device and the port. The device settings are labeled "System." All other settings refer to port settings. For more information on the data presented, refer to the Policy Manager Port Properties Authentication Configuration Tab and Authentication Tab (Device) Help topics. You can enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

## Authentication Sessions

The Authentication Sessions table displays port end user sessions. The Results Filter (accessed through a right-mouse click on a column heading or anywhere in the table body) lets you select the result categories that appear in the table (802.1x, MAC, Web-based, etc.). When the **Active Sessions** checkbox is checked in the Results filter, only your active sessions are displayed. Select an entry in the table to display NAC Manager end-system information for that MAC address, in a line below the table. You can

enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

## 802.1D

This section displays 802.1D bridge and spanning tree information for the port.

### Bridge Filtering Database

This table displays the bridge filtering database for the port. Select an entry in the table to display NAC Manager end-system information for that MAC address, in a line below the table. You can enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

### Node/Alias

This table displays the node/alias entries that match the ifIndex of the port. Select an entry in the table to display NAC Manager end-system information for that MAC address, in a line below the table. You can enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

### MAC Locking

This table displays MAC locking settings for the port. You can enable and disable the display of this data in the Suite-Wide Options Port Monitor Options panel.

- MAC Locking Globally - whether MAC locking is enabled or disabled on the device.
- Port Status - whether MAC locking is enabled or disabled on the port.
- Trap Status - whether MAC lock trap messaging is enabled or disabled on the port.
- Syslog Status - whether MAC lock syslog messaging is enabled or disabled on the port.
- Aging Status - whether MAC lock aging is enabled or disabled on the port.
- Max Static - the maximum number of MAC addresses that can be locked administratively on the port.
- Max First Arrival - the maximum end station MAC addresses allowed locked to the port.
- Last Violating MAC Address - the most recent MAC addresses violating the maximum static and first arrival values set for the port.

## Properties Tab

---

The information in this tab depends on your selection in the left panel and the specific view selected on the Properties tab. When a Device Group is selected, the right panel tab contains tabular information for the group. When a single device is selected, the right panel tab contains only information for the selected device


- [Device Properties](#)
- [Access Properties](#)
- [Date/Time Properties](#)
- [Port Properties](#)

## Properties Tab (Device)

---

Depending on your selection in the left panel, this tab contains either a table listing the information about all the devices within the currently selected group or only the information for the currently selected single device.

When a device or device group is selected from the left panel, the Properties tab shows a table listing information about your selection.

At the top left of the tab, there is a menu button  that provides the following options:

- **Status Poller Options** - opens a window 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.
- **PropView Options** - opens a window where you can specify options that define the SNMP polling parameters and appearance of the Properties tab in Console.

IP Address	Display Name	Device Type	Status	Firmware	Boot PROM	Base
12.22.54.60	12.22.54.60	CSK125-24	Contact Established	06.51.02.0...	02.01.51	00:1F:45:1
12.22.54.61	12.22.54.61	B5K125-24	Contact Established	06.61.05.0...	02.01.50	00:1F:45:2
12.22.54.63	12.22.54.63	K6	Contact Established	07.70.02.0...	01.01.22	00:11:88:1
12.22.54.88	12.22.54.88	XSR-1805	Contact Established	7.6.15.0006	3.2	00:01:F4:1
12.22.80.1	12.22.80.1	SSA-T1068-0652	Contact Established	07.62.01.0...	01.01.00	00:1F:45:1
12.22.80.6	12.22.80.6	Matrix N1 Platinum	Contact Established	06.11.01.0...	01.00.15	00:11:88:1
12.22.80.7	12.22.80.7	1H582-51	Contact Established	03.07.33	01.02.00	00:01:F4:1
12.22.80.9	12.22.80.9	C3G124-24	Contact Established	06.03.04.0...	01.00.49	00:11:88:1
12.22.80.10	12.22.80.10	Matrix N1 Platinum	Contact Established	07.62.01.0...	01.00.19	00:11:88:1
12.22.80.11	12.22.80.11	Matrix N1 Platinum	Contact Established	07.21.03.0...	01.00.16	00:11:88:1
12.22.80.12	12.22.80.12	C3G124-24	Contact Established	06.03.04.0...	01.00.49	00:11:88:1
12.22.80.13	12.22.80.13	C3G124-48	Contact Established	05.02.08.0...	01.00.47	00:11:88:1
12.22.80.15	12.22.80.15	C3G124-24	Contact Established	06.03.04.0...	01.00.49	00:11:88:1
12.22.80.16	12.22.80.16	Enterasys NAC ...	Contact Established	06.11.01.0...	01.00.21	00:11:88:1
12.22.80.80	12.22.80.80	2H252-25R	Contact Established	05.08.04	02.01.06	00:E0:63:1

### IP Address

Device IP Address

### Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

### Device Type

The type of device.

### Status

Current operational status of the device.

### Firmware

The revision for the firmware running in the device.

### BootPROM

The revision for the BootPROM installed on the device.

### Base MAC

The base MAC address for the device.

### Chassis ID

The ID of the chassis containing the device.

### Location

Physical location of the device. Console automatically creates (system-created) sub-groups in the left panel **Grouped By > Location** folder for each level defined by the Location. The specific levels are separated by the **Auto Group Delimiter** defined in Suite-Wide, Data Display - Options view.



### Contact

The name of the responsible contact person.

### System Name

An administratively-assigned hostname for the device taken from the *sysName* MIB object.

### Nickname

User-defined nickname for the selected device. This is the name for this device that will appear in the left panel when the Console's Data Display, **Use User Defined Nickname** option is selected.

### Description

A description of the device.

### User Data 1, User Data 2, Notes

These columns can be edited to provide additional information about the device.

### Table Editor

This row is visible when the Show/Hide Table Editor button is toggled to make the Table Editor visible. Columns that contain a writable MIB object will appear in the Table Editor as an editable field or drop down list as appropriate for the object type (integer, boolean, text, etc.). Changing the value in the Table Editor row alters the value for that entry in the row selected in the table. Clicking **Apply** sets the current writable table values on the devices in the currently selected device group.



### Refresh

This button performs a refresh and rediscover of the devices in the table.



### (Table Editor)


This button toggles the Table Editor, where you can change a value of writable MIB objects in the table.



### (Apply)

This button sets the current writable table values on the devices in the currently selected device group.

### *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 other device related

views and a set of Table Tools that can be used to manage information in the table.

---

## Related Information


For information on related windows:

- [Main Window](#)
- [Access Properties](#)
- [Date/Time Properties](#)
- [Port Properties](#)

## Properties Tab (Access)

---

When a device or device group is selected from the left panel, the Properties tab (with the Access button selected) shows a table listing access information for the selected device or device group. You can also use this table to change a device's poll type and poll group.

At the top left of the tab, there is a menu button  that provides the following options:

- **Status Poller Options** — opens a window 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.
- **PropView Options** — opens a window where you can specify options that define the SNMP polling parameters and appearance of the Properties tab in Console.

IP Address	Display Name	Status	Context	Poll Type	Poll Group	Profile	Timeout	Retries
10.54.22.10	10.54.22.10	Contact Established	Context	SNMP	Default	public_v1_Profile	Default	Default

### IP Address

The device's IP address.

### Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

### Status

Current operational status of the device.

### Context

Context lets you access a subset of MIB objects related to a context that has been configured on the device. Console lets you specify a SNMP Context for both SNMPv1/v2 and SNMPv3.

The use of context differs depending on the protocol version being used with a user's credentials:

- When used with SNMPv3 credentials, the context provides access to a specific collection of MIB objects associated with a particular context configured on the device. If the credentials used are accepted but the context specified doesn't match one configured on the device, access

is denied.

- Some devices also provide limited support of contexts for SNMPv1/v2. For these devices, a SNMPv1 or SNMPv2 credential (community name) can be mapped, through Local Management, to a particular SNMP context on the device. Then, when SNMPv1/v2 credentials are used with a Context entry, access is granted to the subset of MIB objects associated with that context. If the credential used is accepted, but the context specified doesn't match a context configured on the device, access is granted to the default context.

Console treats each context for a given device (IP address) as a distinct device. All SNMP contexts known to the device can be displayed using the `show snmp context` command. Refer to a *Matrix Series Configuration Guide* for more information about setting and showing SNMP contexts.

### Poll Type

Displays the poll type for the selected device: SNMP, Ping, or Not Polled. The poll type is the mechanism that is used to determine the device status (indicated by the green up arrow or red down arrow in the left-panel tree). When the SNMP poll type is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the particular Profile assigned to the device. You can change a device's poll type using the Table Editor.

---

**NOTE:** For a NetSight Server running on a Windows platform, device operational status cannot be determined for devices with their **Poll Type** set to **Ping only** unless the server was launched by a user with Administrative privileges.

---

### Poll Group

The poll group the device is assigned to. Console provides three distinct poll groups with different polling intervals. This allows critical devices to be polled at a more frequent interval, while non-essential devices are polled less frequently. When a device is added to the NetSight database, it is added to the poll group that you have designated as the default poll group. You can reassign devices to a different poll group using the Table Editor. Poll groups are defined in the Suite-Wide options Status Polling panel.

### Profile

The Access Profile that Console is using when attempting to communicate with the device. You can change a device's access profile using the Table Editor here or in the Profile/Device Mapping tab in the Authorization/Device Access tool. You can only change the profile if you are a member of the administrator group, and only the device administrator profile changes, not the profiles for other authorization groups.



## Timeout

The amount of time (in seconds) that Console waits before re-trying to contact the device selected in the device tree. The maximum setting is 20 seconds. The value entered in this field overrides the global default value entered in the **Length of SNMP Timeout (in seconds)** field on the [Advanced SNMP Settings](#) window of the Suite Options window.

## Retries

The number of attempts made to contact the device selected in the device tree after an attempt at contact fails. The value entered in this field overrides the global default value entered in the **Number of SNMP Retries** field on the [Advanced SNMP Settings](#) window of the Suite Options window.

## Table Editor

Use the Table Editor button  to display the Table Editor row at the bottom of the table. The Table Editor lets you change the poll type and poll group values for the devices selected in the table, by clicking on the value in the table editor row and selecting a new value from the drop-down list. After you have made changes, click the Apply button  to set the new values on the devices.

## Refresh

This button performs a refresh and rediscover of the devices in the table.


## Table Editor

This button toggles to display and hide the Table Editor, where you can change the poll type and poll group values in the table.

## Apply

This button applies any changes you have made to the poll type and poll group values for the devices in the table.

## *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 other device related views and a set of Table Tools that can be used to manage information in the table.

## Related Information

For information on related windows:


- [Device Properties](#)
- [Date/Time Properties](#)
- [Port Properties](#)

## Properties Tab (Date/Time)

---

Depending on your selection in the left panel, this tab contains either a table listing the date and time information for all the devices within the currently selected group or only the date and time information for the currently selected single device.

When a device or device group is selected from the left panel, the Properties tab shows a table listing date and time information for your selection.

At the top left of the tab, there is a menu button  that provides the following options:

- **Status Poller Options** - opens a window 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.
- **PropView Options** - opens a window where you can specify options that define the SNMP polling parameters and appearance of the Properties tab in Console.

IP Address	Display Name	Uptime	Date/Time
10.20.33.1	10.20.33.1	Searching	01/12/2005 10:38:33 AM
10.20.33.3	10.20.33.3	Searching	01/12/2005 09:44:40 AM
10.20.33.9	10.20.33.9	Searching	01/12/2005 09:44:54 AM
10.20.33.10	10.20.33.10	Searching	01/12/2005 09:44:54 AM
10.20.33.11	10.20.33.11	Searching	01/12/2005 09:45:19 AM
10.20.33.12	10.20.33.12	Searching	01/12/2005 09:44:34 AM
10.20.33.13	10.20.33.13	Searching	01/12/2005 09:44:34 AM
10.20.33.14	10.20.33.14	15 Days 19:04:03.46	01/12/2005 09:44:25 AM
10.20.33.15	10.20.33.15	Searching	01/12/2005 09:44:35 AM
10.20.33.18	10.20.33.18	N/A <No Contact>	N/A <No Contact>
10.20.33.19	10.20.33.19	Searching	N/A
10.20.150.1	10.20.150.1	Searching	01/12/2005 09:47:48 AM
10.20.150.2	10.20.150.2	Searching	01/12/2005 09:53:16 AM
10.20.150.75	10.20.150.75	Searching	N/A
10.20.150.76	10.20.150.76	Searching	01/12/2005 09:37:37 AM
10.20.150.77	10.20.150.77	Searching	01/12/2005 09:45:01 AM
10.20.150.78	10.20.150.78	Searching	01/12/2005 09:54:05 AM
10.20.150.79	10.20.150.79	1 Day 22:37:15.16	01/12/2005 09:51:01 AM
10.20.150.80	10.20.150.80	Searching	01/12/2005 09:52:00 AM

## IP Address

Device IP Address

## Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

## Uptime

The elapsed time since the last time this device was re-booted.

## Date/Time

The date and time retrieved as of the last poll.


## Table Editor

This row is visible when the Show/Hide Table Editor button is toggled to make the Table Editor visible. Columns that contain a writable MIB object will appear in the Table Editor as an editable field or drop down list as appropriate for the object type (integer, boolean, text, etc.). Changing the value in the Table Editor row alters the value for that entry in the row(s) selected in the table. Clicking **Apply** sets the current writable table values on the device(s) in the currently selected device group.



## Refresh

This button performs a refresh and rediscover of the devices in the table.

 **Table Editor (Edit Date/Time)**

This button toggles the Table Editor row. You can select one or more table rows where you want to change the date/time for device(s). Clicking in the Table Editor row for the Date/Time column opens the Change Date/Time window, where you can set a specific date and time to be set in the selected device(s). When the the date/time are changed on a device, a green exclamation mark appears in that row to indicate that the new value needs to be applied.


 **(Apply)**

This button sets the current writable table values on the devices in the currently selected device group.

 **(Retrieve)**

This button attempts to contact the selected device or device group to update the table information. The Properties view uses the Profile for the Read Access Level of the customizations for the current user. While retrieving information the button changes to a red octagon.

### *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 other device related views and a set of Table Tools that can be used to manage information in the table.

---

### **Related Information**

For information on related windows:

- [Main Window](#)
- [Access Properties](#)
- [Device Properties](#)
- [Port Properties](#)

### **Properties Tab (Ports View)**


---

This tab lists port information for a device, device group, or port element, depending on your selection in the left-panel device tree. The first time you

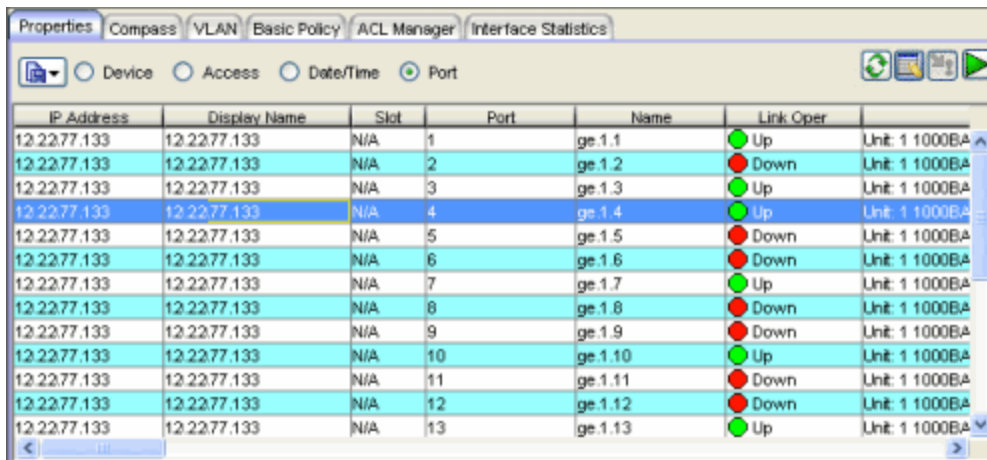


access the Port Properties tab the table is blank and you must click the  Retrieve button to display port information.

**IMPORTANT:** The Port Properties table is not automatically updated. Instead, the table must be refreshed using the Retrieve button to update the table information each time you access this tab. For example, if you leave the Port Properties tab and then return, the contents of the table will not have changed, even though conditions on device ports may have changed. You must retrieve the information again to get the latest data.

At the top left of the tab, there is a menu button  that provides the following options:

- **Status Poller Options** - opens a window 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.
- **PropView Options** - opens a window where you can specify options that define the SNMP polling parameters and appearance of the Properties tab in Console.



IP Address	Display Name	Slot	Port	Name	Link Oper	Unit
12.22.77.133	12.22.77.133	N/A	1	ge.1.1	Up	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	2	ge.1.2	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	3	ge.1.3	Up	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	4	ge.1.4	Up	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	5	ge.1.5	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	6	ge.1.6	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	7	ge.1.7	Up	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	8	ge.1.8	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	9	ge.1.9	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	10	ge.1.10	Up	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	11	ge.1.11	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	12	ge.1.12	Down	Unit: 1 1000BA
12.22.77.133	12.22.77.133	N/A	13	ge.1.13	Up	Unit: 1 1000BA

### IP Address

The IP address of the device and, when applicable the SNMP Context.

### Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

**Slot**

The range of ports in some devices span multiple slots. For these devices, this column shows the board location (slot) within the chassis where the port is located.

**Port**

The port number (ifIndex).

**Name**

The interface name for the port.

**Link Oper**

Displays the status of the port's connection (link) with a remote port: **Up**, **Down**, **Dormant**, etc..

**Description**

A description of the port.

**Alias**

Shows the alias (ifAlias) for the interface.

**Port Type**

The interface type for the port.

**MTU**

The size of the largest packet (in octets) that can be sent or received on the port.

**Bandwidth**

An estimate of the port's current bandwidth in bits per second.

**MAC Address**

The port's MAC Address.

**Link Admin**

Configures the status of the port's connection (link) with a remote port: **Up**, **Down**, or **Testing**.

**Statistics**

These columns show port traffic statistics. These columns are hidden or displayed according to your selection from the [Column Filter](#) toolbar.

**Last Change**

The System Up Time at the time of the last change to the operational status for the port.

**In Octets**

Displays the number of octets received on the port.

**In Ucast Pkts**

Displays the number of packets received on the port that had a single, unique source or destination address.

**In Discards**

The number of packets received on the port that were chosen to be discarded, even though no errors were detected.

**In Errors**

The number of packets received that contained errors.

**In Unknown Packets**

The number of packets received that were discarded because of an unknown or unsupported protocol.

**Out Octets**

Displays the number of octets transmitted on the port.

**Out Ucast Pkts**

Displays the number of packets transmitted on the port that had a single, unique source or destination address.

**Out Discards**

The number of packets transmitted on the port that were chosen to be discarded, even though no errors were detected.

**Out Errors**

The number of packets that could not be transmitted because of errors.

**Configuration**

These columns can be used to configure auto negotiation for selected port (s). If auto negotiation is disabled, you can manually configure the speed, duplex, and flow control parameters of the selected port(s). These columns are hidden or displayed according to your selection from the [Column Filter](#) toolbar.

To configure parameters on multiple ports, enable the Table Editor and select the ports in the table by swiping with your mouse or using the Ctrl or Shift keys. The information for the first port selected will be displayed in the Table Editor row. Any changes that you make will be applied to all of the selected ports. Use the drop-down lists in the Table Editor row to manually

configure the parameters when auto negotiation is disabled on the selected port(s).

---

**NOTE:** If you manually configure these parameters, be sure that the remote port supports the same mode. Otherwise, no link between the local and remote port will be achieved.

---

### Remote Auto Signal

Indicates whether auto negotiation signaling is detected on the remote port: **Detected** or **Not Detected**.

### Auto Negotiate Config

Indicates whether auto negotiation signaling is in progress (**Configuring**) or has completed (**Complete**).

### Auto Negotiate

Displays whether auto negotiation is enabled or disabled on the port.

### Speed Oper

Displays the current operational speed for the port.

### Speed Admin

Configures the speed for the port when it is not set to auto negotiation.

### Duplex Oper

Displays the current duplex mode for the port: **Half Duplex** or **Full Duplex**.

### Duplex Admin

Configures the duplex mode for the port when it is not set to auto negotiation: **Half Duplex** or **Full Duplex**.

### Flow Control Columns

Displays the current flow control method that the port uses to notify the remote port that congestion is occurring and that the sending device should stop transmitting until the congestion can be cleared.

### Full Duplex Flow Control Oper

Displays the flow control method for the port.

### Full Duplex Flow Control Admin

Configures the flow control method for the port.

- Enabled -- Enables flow control on the port.
- Disabled -- Enables flow control on the port.

- Enabled Transmit -- Configures the port to send pause control frames, but does not acknowledge received pause control frames. This option is only available for Gigabit Ethernet ports.
- Enabled Receive -- Configures the port to receive pause control frames, but does not transmit its own. This option is only available for Gigabit Ethernet ports.
- Enabled Transmit and Receive -- Configures the port to both receive and transmit pause control frames.
- Auto Negotiate -- Configures the port to only uses pause control frames if the negotiation process determines that the remote port supports them. Both ends of the link must support auto negotiation and a common mode of operation.

#### Half Duplex Flow Control Oper

Displays the flow control method for the port when.

#### Half Duplex Flow Control Admin

Configures the flow control method for the port when it is not set to auto negotiation.

- Enabled -- Enables flow control on the port.
- Disabled -- Enables flow control on the port.

#### Capabilities

These columns display the operational modes that are supported by the local and remote ports and the specific operational modes, supported by the local port, that are being advertised to the remote port. These columns are hidden or displayed according to your selection from the [Column Filter](#) toolbar.

---

**NOTE:** This section does not apply if you have manually configured specific operational modes for your 100Base-TX port, or if you are configuring a 100Base-FX port.

---

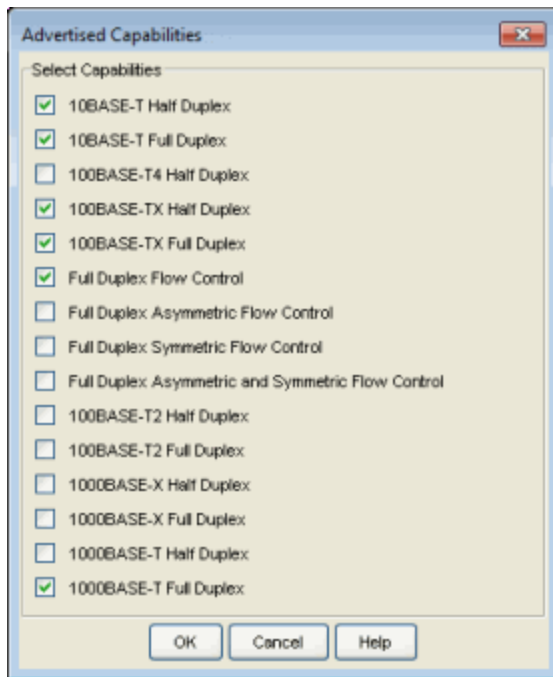
#### Advertised Capabilities

Indicates the local port's advertised ability for each specific operational mode. The advertised ability only becomes active on ports that have auto negotiation enabled. Displays whether an operational mode is advertised to the remote port. Only those modes supported by the local port can be advertised. The table lists the currently advertised capabilities as a comma-separated string.

**Advertised Capabilities Window** With the Table Editor enabled, clicking in the editor row for this column opens the Advertised Capabilities window. This window lets you selectively advertise capabilities for one or more ports selected in the table.

**Checked** -- Indicates that the mode is being advertised.

**Un-checked** -- Indicates that the mode is not being advertised.



### Local Capabilities

Indicates whether the local port's hardware capability supports each specific operational mode.

### Remote Capabilities

Indicates the remote port's advertised ability for each specific operational mode.

### Table Editor

This row is visible when the Show/Hide Table Editor button is toggled to make the Table Editor visible. Columns that contain a writable MIB object will appear in the Table Editor as an editable field or drop down list as appropriate for the object type (integer, boolean, text, etc.). Changing the value in the Table Editor row alters the value for that entry in the row(s) selected in the table. Clicking **Apply** sets the current writable table values on the device(s) in the currently selected device group.

**Refresh**

This button performs a refresh and rediscover of the devices in the table.

**(Table Editor)**

This button toggles the Table Editor, where you can change the value of writable MIB objects in the table.

**(Apply)**

This button sets the current writable table values on the devices in the currently selected device group.

---


**CAUTION:** Applying certain MIB objects can disable devices and cause interruptions to network operation. Do Not apply MIB values unless you are sure of the outcome.

---

**(Retrieve)**

This button attempts to contact the selected device or device group to update the table information. The Properties view uses the Profile for the Read Access Level of the customizations for the current user. While retrieving information the button changes to a red octagon.

### *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 other device related views and a set of Table Tools that can be used to manage information in the table.

---

### **Related Information**

For information on related windows:

- [Device Properties](#)
- [Access Properties](#)
- [Date/Time Properties](#)

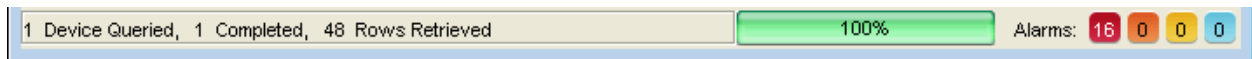
## Status Bar

---

The status bar at the bottom of the Console main window provides operational information as text messages and a progress bar. The text messages show the results of recent Console operations, for example a Discovery operation. The progress bar indicates the level of completion during the performance of a Console operation.

The status bar also displays a system-wide alarm summary that indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) present in the entire system. If there are no current alarms, the status will read all zeroes. Click on an indicator to view details on the alarms with that severity.

### *Sample Status Bar*



---

## Related Information

For information on related windows:

- [Main Window](#)
- [Menu Bar](#)
- [Tool Bar](#)
- [Left Panel](#)
- [Right Panel](#)



## Syslog Receiver Configuration Window

---

Syslog Receivers are systems on your network where a Syslog server has been installed. This window lets you set the IP addresses for those Syslog Receivers on your network devices so that the devices in your network will know where to send Syslog messages.

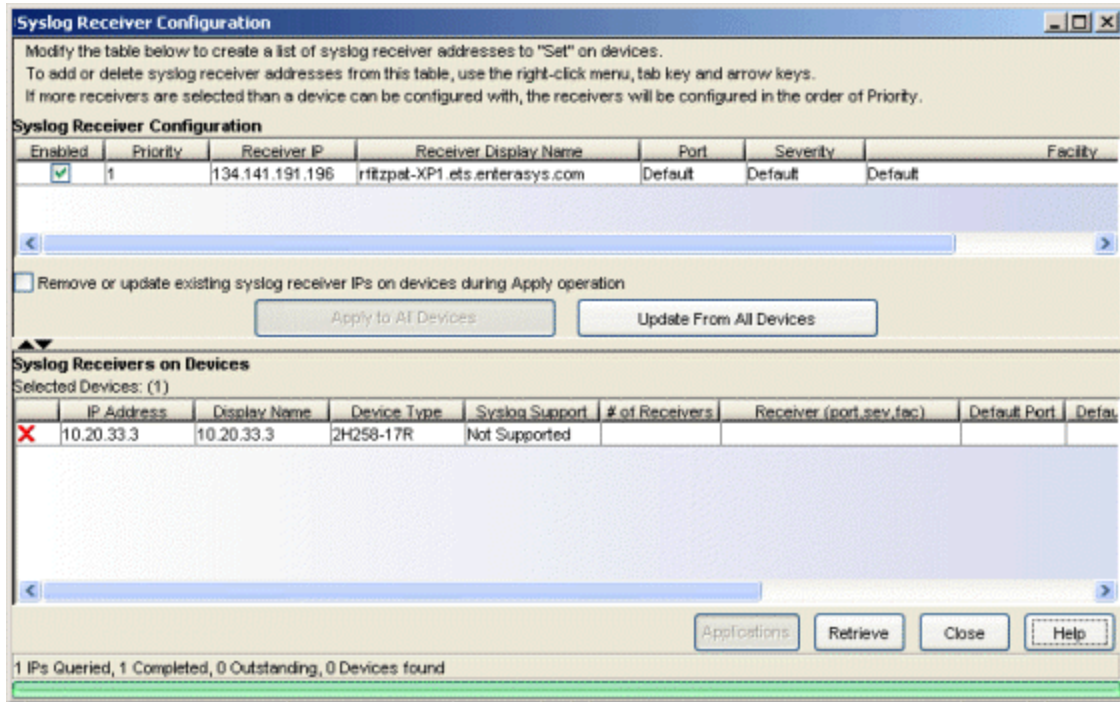
The Syslog Receiver Configuration window is accessed from the right-click menu when one or more devices is selected in the left panel of the Console's main window. The **Syslog Receivers on Devices** table in the lower half of the window is automatically populated with the IP address(es) of your selection(s) from Console's left panel when the Syslog Receiver Configuration window is opened. The **Syslog Receiver Configuration** table in the upper half of the window lists the workstation where the Console server is running.

---

**CAUTION:** When there are multiple installations of NetSight Console on your network, it is possible for another Console to be altering device Syslog receiver configuration settings at the same time. To reduce the possibility of configuration conflicts you should **Retrieve** the current Syslog receiver settings and check for conflicts prior to applying (**Apply to All/Selected Devices**) your specific Syslog receiver configuration settings.


After retrieving the current settings, you must select specific devices (or all devices) before you can apply settings. In spite of this precaution, there remains a remote chance that changes applied between retrieving and applying will overwrite changes made from another Console.

---



### Syslog Receiver Configuration Table

This table shows a listing of Syslog receivers configured in your network devices. Initially, the table is populated with the Console management station's information. Clicking the Update from Devices updates the table to include information for all the Syslog receivers that have been configured on all the currently selected devices. When the Syslog Receiver Configuration window is initially opened, this table lists information for the Console server workstation. You can click **Update From All/Selected Devices** to include information for all the Syslog receivers that have been configured on all the currently selected devices. You can also add Syslog receivers manually to the table by right-clicking on an existing row and selecting **Insert Row** (Tabbing past the last row will also create a new row.). The new row is created above the selected row using the same parameters. Double clicking the fields in the new row allows you to edit their content.

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 a set of Table Tools that can be used to manage information in the table.

### Enabled

When checked the **Apply to All/Selected Devices** button will set the associated Syslog receiver information on the all/selected devices.

### Priority

Determines the order in which Syslog Receiver information will be set on the selected devices, with the lower numbers taking precedence. **Apply to All/Selected Devices** writes Syslog receiver IPs to each device in order, starting with the lowest receiver number until all are written or a device cannot accept any more. An **Update From All/Selected Devices** operation returns Syslog receiver information from the selected/all devices. The status shows a count of all of the Syslog receivers returned.

### Receiver IP

The IP address for a Syslog receiver (the system where devices will send Syslog messages). Valid Syslog receivers are systems running a Syslog Server.

### Receiver Display Name

The hostname for the Syslog Receiver system where devices will send Syslog messages.

### Port

The default UDP port the client uses to send to the Syslog Receiver system.

### Severity

The minimum severity level at which the Syslog Receiver system will accept Syslog messages. Valid values and corresponding levels are: Default, 1 - emergencies (system is unusable), 2 - alerts (immediate action required), 3 - critical conditions, 4 - error conditions, 5 - warning conditions, 6 - notifications (significant conditions), 7 - informational messages, 8 - debugging messages.

### Facility

The Syslog Receiver's facility name. Valid entries are: default, or local0 to local7.

### Remove or update existing syslog receiver IPs on devices during Apply operation

When checked, an Apply operation will attempt to make the Syslog Receiver Configuration table on the devices match the enabled entries in the Syslog Receiver table, by adding and removing entries.




When unchecked, an Apply operation will attempt to add entries from the Syslog Receiver Configuration table, that don't already exist on a device, to the devices Syslog Receiver table. Entries existing on devices are not modified in any way and no redundant addresses are created on the devices.

### Syslog Receivers on Devices Table

This table lists the devices that were selected from the left panel in Console's main window when the Syslog Receiver Configuration window was opened. It shows the Syslog Receiver information configured on the selected device(s).

### Status Icon

The status icon for the selected device indicates the following conditions:

- Blank - Either the row is not selected or that the syslog receivers configured on the device match the syslog receiver table list
-  - Indicates that an "Apply" operation will cause changes to be made to this device, and that all selected Receivers should be able to be configured on the device.
-  - Indicates that the device has a warning status that will interfere with application of the enabled syslog receivers to this device. The status column will indicate the reason for the warning. (includes stopped and not supported).
-  - Indicates that the device has a warning status that will interfere with application of the enabled syslog receivers to this device. The status column will indicate the reason for the warning. (includes stopped and not supported).

### IP Address

The IP address of the selected device.

### Display Name

The name that appears in the left panel of the main window that is associated with this device, according to your current Suite-Wide Data Display Options setting.

### Device Type

The model name for the selected device.

### Syslog Support

Supported/Not Supported, indicates whether or not a Syslog application is supported by the selected device.

### # of Receivers

The number of IP addresses detected in the Syslog Receivers table on the selected device.

### Receiver port, sev, fac

This is a semicolon separated list showing the current Syslog settings in the selected device(s).

### Default Port, Severity, Facility

The default UDP port, minimum severity level, and facility name currently configured on the selected device(s). These defaults are set by the **set logging defaults** command in the selected device(s).

### Status

Shows the current status of **Apply** or **Update** operations:

- **Reading - Update From All/Selected devices** in progress
- **Complete** - Update or Apply finished
- **Setting - Apply to All/Selected devices** in progress
- **Error** - Operation unsuccessful for the device (e.g., no such name, insufficient access level, request timed out, etc.) Details are also recorded in Event log
- **Warning** - Operation partially successful. This can occur when Syslog receiver configuration is not supported or has a limitation in the selected device (e.g., Syslog Receiver configuration not supported, Syslog Receiver Table Full, Not enough room to store all Syslog receivers).

### Applications Button

This button lets you configure logging applications on a (single) device selected from the **Syslog Receivers on Devices** table. It opens the [Syslog Applications](#) window where you can define the severity associated with each syslog application and identify the servers that will be notified.

### Apply to All/Selected devices Button

This button changes depending on whether or not devices have been selected from the **Syslog Receivers on Devices** table. With no devices selected the operation is performed on all devices. Apply operations write (set) Syslog Receiver IPs listed in the Syslog Receiver table to the selected devices.

### Update From All/Selected devices Button

This button changes depending on whether or not devices have been selected from the **Syslog Receivers on Devices** table. With no devices selected the operation is performed on all devices. Update operations

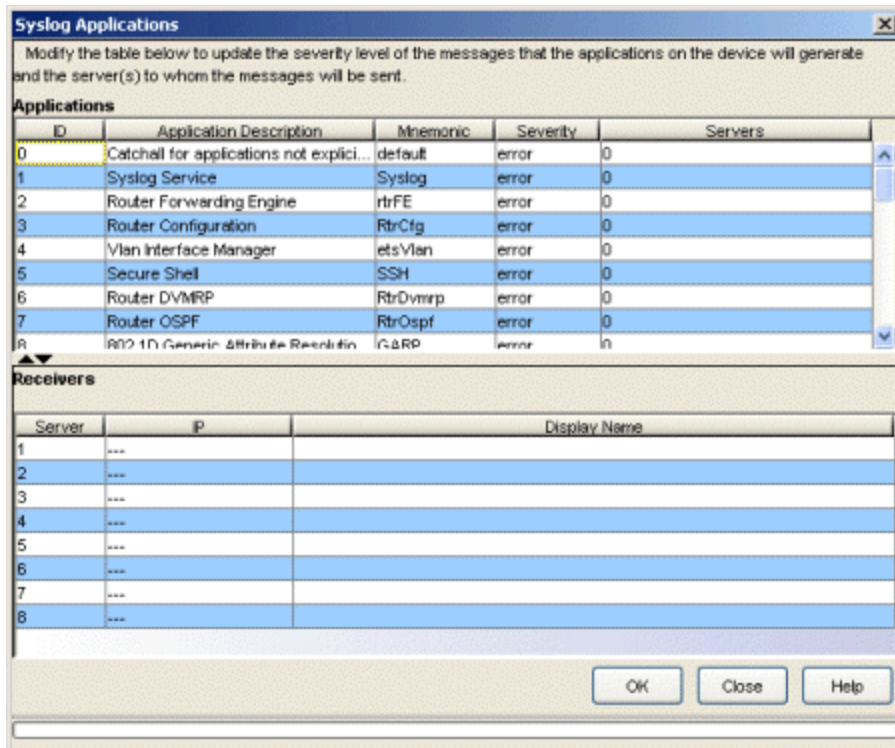
retrieve the trap receiver table from the devices and update the information in the Syslog Configuration table.

**Retrieve Button**

Updates the information in the **Syslog Receivers on Devices** table.

**Syslog Applications Window**

When a device is selected in the **Syslog Receivers on Devices** table, this window lets you define the severity levels associated with each syslog application and identify the servers that will be notified. Console reads the Syslog information from the selected device when the window is initially opened and populates the [Applications](#) table with the application information and syslog receivers currently configured on the device. The Severity and Servers columns in the Applications table can be edited.



**Applications**

This table contains the application information currently configured on the selected device. The Severity and Servers columns can be edited to define the severity for each of the associated applications and which Server(s) should receive the associated syslog message. Double-clicking in a table cell allows editing the information.

- **Severity** - selections are available from a drop-down list: emergencies, alerts, critical, error, warning, notice, info, debug, Default.
- **Servers** - entries identify the entry(ies) from the Receivers table that should receive syslog messages for the associated severity. Servers are referenced here by Server (index) number and can be entered in any of the following formats:
  - Server (index) number
  - Comma delimited list (e.g., 1,4,5)
  - Range of Servers (e.g., 1-5)
  - Combination of above formats (e.g., 1,3, 5-7)

### Receivers

This is a list is retrieved from the Syslog Receiver table in the selected device when the Syslog Applications window is initially opened. It cannot be edited, but rather, provides a reference for the available Syslog servers.

## Main Window - Toolbar

---

The toolbar on the Console main window provides easy access to some of the more commonly used Console functions. Some toolbar buttons may not be available, depending on your current selection within the Console application. Pausing with your mouse pointer over the toolbar icons displays tool tips showing the button's function.



### Exit

Closes the Console application. This button serves the same function as the **File > Exit** menu option.

### Cut

Removes the currently selected items and places them on a clipboard. This button serves the same function as the **Edit > Cut** menu option.

### Copy

Copies an item selected in the left or right panel. The button may or may not be available, depending on where you are in the application. This button serves the same function as the **Edit > Copy** menu option.

### Paste

Pastes what has been cut or copied into the specified location. The button may or may not be available, depending on where you are in the application. This button serves the same function as the **Edit > Paste** menu option.

### Delete

Deletes the device selected in the Console device tree.

### Authorization/Device Access

Opens the Authorization/Device Access window where you can define users and groups and configure their access to features available in NetSight applications. This button serves the same function as the **Tools > Authorization/Device Access** menu option.

### Server Information

Opens the Server Information window where you can view and configure certain NetSight Server functions, including management of client



connections, locks, and licenses. This button serves the same function as the **Tools > Server Information** menu option.

### Discover

Opens the Discover tool where you can discover devices on your network and populate the NetSight database.

### Wireless Manager

Launches Wireless Manager, a tool that enables you to configure and manage multiple ExtremeWireless wireless controllers and their associated wireless APs.

### Alarms Manager

Launches the [Alarms Manager window](#) where you can configure the network alarms that provide status information for a particular problem or condition on a particular network component.

### Add FlexView Tab

Adds a new FlexView tab in the right panel. The new tab appears with the title of the last FlexView accessed, but once the tab is added you can select a specific FlexView and its title will appear on the tab. This button serves the same function as the **FlexView > Add FlexView Tab** menu option.

### Remove FlexView Tab

Deletes the currently selected FlexView tab from the right panel. This button serves the same function as the **FlexView > Remove FlexView Tab** menu option.

### About this Window

Opens the NetSight Help system to information about the currently selected window.

---

## Related Information

For information on related windows:

- [Main Window](#)
- [Menus](#)
- [Left Panel](#)
- [Right Panel](#)
- [Status Bar](#)

## TopN Collector Advanced Settings Window

---

Use this window to configure advanced settings for the TopN Collector. You can access the window from the [TopN Collector view](#) in the Console options.

The TopN Collector collects the data used in Extreme Management Center TopN reports. It also collects the signal strength data reported by Wireless Controllers. The collector collects data over a one hour time period. At the end of the hour, the collector evaluates the data and stores only the most significant details collected for that hour.

You can use these advanced settings to enable and disable the collection of different TopN data. Enabling and disabling collection will take effect immediately.

You can specify the number of entries to save at the end of each hourly interval. You can also control the amount of memory used during the hour to collect information, by specifying a maximum number of entries. If more entries are needed during the hour than the maximum, additional entries are stored on disk, which is slower. This results in a direct trade-off in memory usage versus CPU usage. Increasing these values might use more memory and decreasing these values might use more CPU.

If you change the value for Number of Entries to Persist (TopN), the new value will be used for the next hourly calculation. For example, if you change the value at 3:05 or 3:55, the new value will be used for the 4:00 calculation.

If you change the value for Maximum Number of Entries in Memory, the new value takes effect during the next hour of data collection. For example, if you change the value at 3:05 or 3:55, it takes effect during the hour that starts at 4:00 and ends at 5:00.

The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1000. The default maximum number of entries in memory is 10000 with a minimum value of 1000 and a maximum value of 1,000,000.



## Trap Receiver Configuration Window

---

Use this window to configure the information needed to receive trap information from the devices on your network. The window has two tabs. The Configuration tab lets you create a list of trap receiver addresses. These are the addresses of the systems that will receive trap information from your network devices. The snmptrapd tab is where you configure the information that is required to allow the NetSight SNMP Trap Service (snmptrapd) to receive **Trap** and **Inform** messages from your network devices that are using SNMPv3.

To access this window, right-click on one or more devices in the Console left-panel tree and select Trap Receiver Configuration.

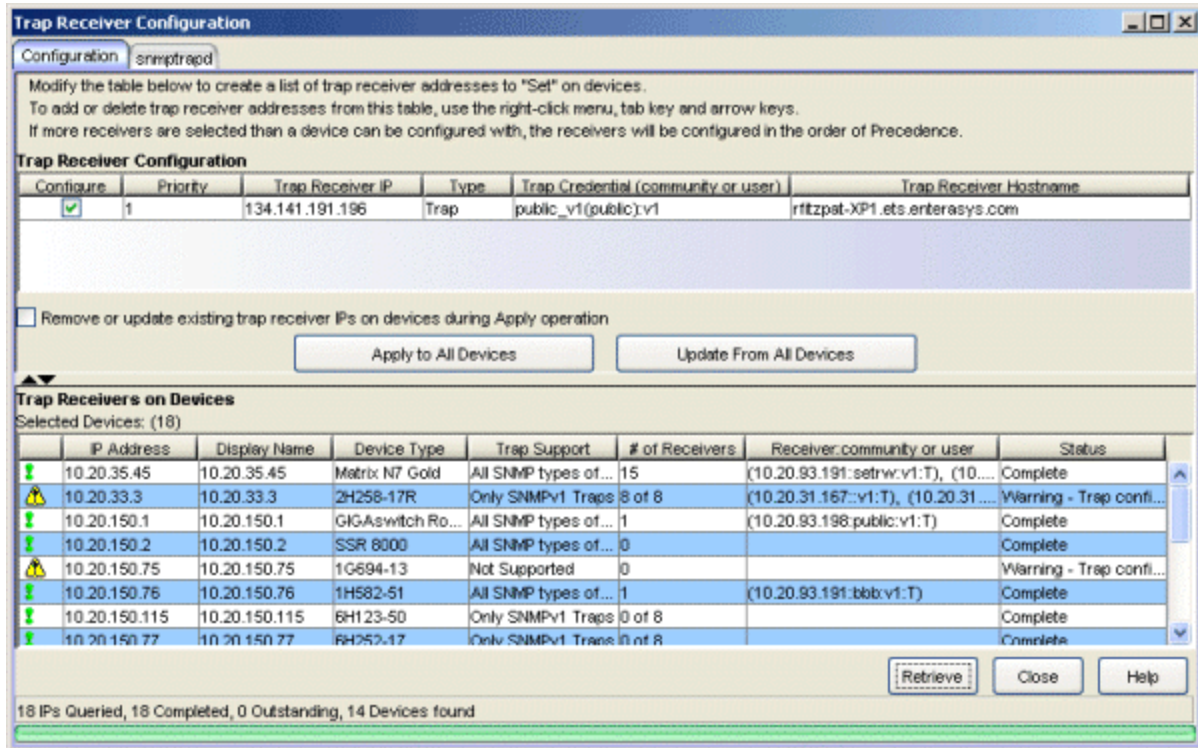
### Configuration Tab

---

**CAUTION:** When there are multiple installations of NetSight Console on your network, it is possible for another Console to be altering device trap configuration settings at the same time. To reduce the possibility of configuration conflicts you should **Retrieve** the current trap receiver settings and check for conflicts prior to applying your specific trap receiver configuration settings.

After retrieving the current settings, you must select specific devices (or all devices) before you can apply settings. In spite of this precaution, there remains a remote chance that changes applied between retrieving and applying will overwrite changes made from another Console Trap Receiver Configuration window.

---



## Trap Receiver Configuration Table

Use this table to create a list of trap receiver addresses to apply to your devices. When the Trap Receiver Configuration window is initially opened, this table lists the Console workstation as the only trap receiver. Click the **Update From All/Selected Devices** button to update the table with trap receiver information from the selected devices. You can also manually add trap receivers to the table. To add a new trap receiver, right-click on an existing row and select Insert Row. A new row will be created above the selected row. (Tabbing past the last row will also create a new row.) Tab through the table columns and modify each entry as desired.

## Configure

Check this checkbox if you want this particular trap receiver entry to be set on the selected devices when you **Apply** your trap receiver configuration settings.

## Priority

Use this column to specify the order in which trap receiver entries will be set on the selected devices, with the lowest number having the highest priority. When you **Apply** your trap receiver settings, Console writes the Trap Receiver IPs to each device in order, starting with the highest priority

(the lowest number) until all are written or a device cannot accept any more.

**Trap Receiver IP**

The IP address for a trap receiver (the system where devices will send traps). Trap receivers systems must be running an SNMPTrap Service.

**Type**

Select the supported message type: Trap, Inform, or Both.

**Trap Credential (community or user)**

The credential used by the device when sending traps. This field will contain a community name when the device is using an SNMPv1/2 credential or a user name for an SNMPv3 credential. The information is displayed in the following format:

*credential(community name or user name):snmp version*

where *credential* is the credential name in Console that uses the *community name* or *user name* (within parentheses), and the *snmp version* which is either v1, v2c, or v3.

When the credential appears within angle brackets (< *credential name* >), it indicates that the community or user name could not be found among the credentials created in Console. When this happens, a temporary credential name is created, derived from the community or user name on the device. For example, if the community name on the device is **security**, and there is no credential in Console with that community name, this column will show <security> as the credential. If a second device is found with the community or user name **security**, its temporary credential will be displayed as <security-2>.

---

**NOTE: E1 devices:** If you have set the **Trap Credential** to the community name set on the device and cannot receive traps, it is because you must use the Security\_User\_Name that is mapped to the community name in the device.

E1 devices map the SNMPv1 community name (by default *public*) to the Security\_User\_Name (by default, *initial*). To determine the mapping in a particular device, use the device Local Management (CLI), **show snmp community** command to determine the Security\_User\_Name associated with the community name. Then, enter the Security\_User\_Name as the **Trap Community**.

---

**Trap Receiver Hostname**

The hostname for the trap receiver system. This column cannot be edited.

**Remove or update existing trap receiver IPs on devices during Apply operation**

When checked, an Apply operation will update the Trap Configuration table on the devices to match the enabled entries in this table, by adding, modifying (updating community names), and removing entries as necessary. Entries on the device that were created via CLI are never deleted or modified.




When unchecked, an Apply operation will add entries from this table to the devices Trap Configuration table. Existing entries on the devices are not modified in any way and no duplicate addresses are created.

**Trap Receivers on Devices Table**

This table lists the devices that were selected in the Console left-panel tree when the Trap Receiver Configuration window was opened, and their trap receiver information.

**Status Icon**

The status icon for the selected device indicates one of the following conditions:

-  - an **Apply to All/Selected devices** operation will apply trap receiver configuration settings to this device.
-  - the device has a warning status that will interfere with the application of some or all of the enabled trap receivers to this device. The status column will indicate the reason for the warning (Not Supported, Unable to Contact, Configuration Table Full, or Not Enough Room in Configuration Table, etc.).
-  - this device will be excluded or has been excluded from an operation. The status column will indicate the reason (Stopped or an error occurred while attempting to **Apply**).
- Blank - either the row is not selected or the trap receivers configured on the device match the trap receiver table list.

**IP Address**

The IP address of the selected device.

**Display Name**

The name displayed for this device in the Console left-panel tree.

**Device Type**

The model name for the selected device.

### Trap Support

Indicates whether trap configuration is supported by the selected device:  
Supported/Not Supported.

### # of Receivers

The number of trap receiver IP addresses detected on the selected device.

### Receiver (community or user)

This is a comma-separated list of the information for each of the trap receivers configured on the device when the Trap Receiver Configuration window was opened. The information is formatted as follows:

*(ip address(community name or user name):snmp version:type)*

where:

*ip address* - the IP address of the trap receiver.

*credential* - the credential name being used with the trap/inform message.

*snmp version* - either v1, v2c, or v3.

*type* - the type of message: I for informs, T for traps.

### Status

Shows the current status of **Apply** or **Update** operations:

- **Reading - Update From All/Selected devices** in progress
- **Complete** - Update or Apply finished
- **Setting - Apply to All/Selected devices** in progress
- **Error** - Operation unsuccessful for the device (e.g., no such name, insufficient access level, request timed out, etc.) Details are also recorded in Event log
- **Warning** - Operation partially successful. This can occur when trap receiver configuration is not supported or has a limitation in the selected device (e.g., Trap Receiver configuration not supported, Trap Receiver Table Full, Not enough room to store all trap receivers)

### Apply to All/Selected devices Button

Apply operations write (set) the trap receiver IPs listed in the Trap Receiver Configuration table to the selected devices. This button changes depending on whether or not devices are selected (highlighted) in the Trap Receivers on Devices table. With no devices selected, the operation is performed on all devices.

### Update From All/Selected devices Button

Update operations retrieve the current trap receiver information from the devices and add it to the Trap Receiver Configuration table. This button changes depending on whether or not devices have been selected in the



Trap Receivers on Devices table. With no devices selected, the operation is performed on all devices.

### Retrieve Button

Retrieves the latest trap receiver information from the devices and updates the Trap Receivers on Devices table.

## snmptrapd Tab

Use this tab to configure the information that is required to allow NetSight's SNMP Trap Service (snmptrapd) to receive **Trap** and **Inform** messages from your network devices that are using SNMPv3.

- 
- NOTES:**
1. Changes that you make in this window alter the `snmptrapd.conf` file. The `snmptrapd.conf` file is located on the server in the `<install directory>\NetSight\appdata` directory. After making changes, you must restart the SNMPTrap Service on the NetSight Server. Refer to [How to Configure the SNMP Trap Service](#) for more information on [restarting the SNMPTrap Service](#).
  2. The `snmptrapd.conf` file is not preserved during the Console Uninstall.
- 

- **Inform** messages require only a User ID and Credentials for a user configured on the device. You should not configure an Engine ID for devices sending Inform messages.
- **Trap** messages require a User ID and Credentials for a user configured on the device, as well as the Engine ID of the SNMPv3 agent running on the device. You must configure an Engine ID for each device that will be sending SNMPv3 Trap messages.

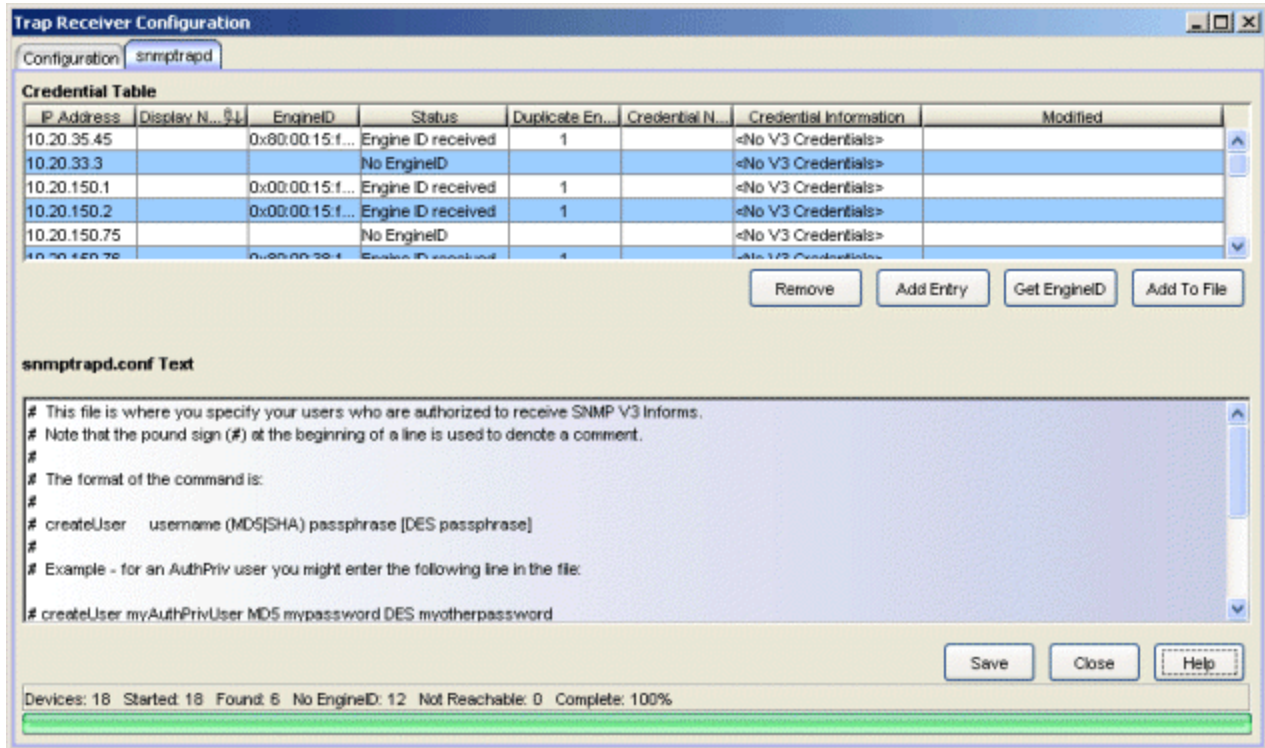
If this information is not provided as part of the SNMP Trap Service configuration, Inform messages are dropped by the SNMP Trap Service. They do not appear in the Console's Trap/Event log and they are not acknowledged by the SNMP Trap Service.

---

**NOTE:** When configuring the SNMP Trap Service to receive Trap messages from an **Extreme Networks IPS** device, the User ID, Credentials, and Engine ID must match the Security Name, Auth Password/Priv Password, and Security Engine, respectively.

Do not use the Engine ID returned by the Extreme Networks IPS device in response to the query that is performed when the snmptrapd Configuration window is opened.

---



## Credential Table

The process for obtaining the information presented in the Credential Table is as follows. When you open the Trap Receiver Configuration window and select the snmptrapd tab, the devices you have selected in the Console left-panel tree are queried for their Engine IDs. A Ping and a SNMPv1 `sysUpTime` request are also sent. If a device does not respond to the Engine ID query, but responds to a Ping or `sysUpTime`, then the device is determined to be a non-SNMPv3 device. The information from the current snmptrapd.conf file is also read and stored. As Engine IDs are returned from the devices, they are compared with the entries already in the table to see if the Engine ID has been configured previously.

As information from the network is returned, the Credential table is updated. The **Credential Name** column can be edited by clicking on the column to display a drop-down list that contains all SNMPv3 credentials from the NetSight database. Once edits are made, the table is updated and an asterisk is displayed in the **Modified** column to show which rows were changed. The configuration file is not updated when the table is edited. Instead, the **Save** button must be used to update the configuration file with any changes that have been made. Closing the window without saving discards the changes.

### IP Address

When the Trap Table is initially opened, the IP Address column lists the IP addresses for all the devices selected in the left-panel tree. This column will be blank when entries are manually added using the **Add Entry** button.

### Display Name

The name that will be displayed for this device in Console's left-panel tree. The display name can be set in the Suite-Wide Options window to the device's **IP Address**, **System Name**, or **Nickname**.

### Engine ID

This column lists the Engine ID of the SNMPv3 agent associated with the selected device(s). This entry is blank when the Status is reported as **In progress**, **No EngineID**, or **Not Reachable**. The Engine ID column is also blank if no Engine ID is supplied when entries are manually added using the **Add Entry** button. To enter an Engine ID for a manually added entry, double-click the Engine ID cell, and type an Engine ID followed by **Enter**.

### Status

This column displays information about the associated device. Potential status entries include:

- **In progress** - An Engine ID query, Ping and `sysUpTime` query are in progress. This status appears when the window is initially opened or for a short time after clicking the **Get Engine ID** button.
- **No EngineID** - The query for the Engine ID has timed out for the associated device, but a response to either the Ping or the SNMPv1 `sysUpTime` request was received. The associated device is not configured for SNMPv3.
- **Engine ID received** - An Engine ID was received from the associated device and it does not match any entry in the configuration file. The same Engine ID may be associated with more than one device. The Duplicate Engine ID column indicates the number of devices sharing a particular Engine ID.
- **In the file** - An Engine ID was received from the associated device, and it matches an entry in the `snmptrapd.conf` configuration file.
- **Not reachable** - All requests (Engine ID, Ping, and `sysUpTime`) to the IP Address have timed out.
- **Added by user** - This status appears when rows are added using the **Add Entry** button.

### Duplicate Engine ID

Some devices can have multiple IP Addresses sharing the same Engine ID. This column shows the number of IP addresses sharing the Engine ID returned from the associated device.

### Credential Name

This column shows the credential of the SNMPv3 agent that is the source of the Trap or Inform information in the device. In the case of Trap messages, when there is an Engine ID in the row and that Engine ID already exists in the configuration file, then the credential associated with the Engine ID in the file will be compared against the one assigned to the device in the NetSight database. If the credential is the same, the credential and Engine ID from the device will be used to identify the device sending traps or inform messages. If the credential does not match, a new credential will be created with a unique name, and it will appear in the Credential Name column. Saving the trap information will add the new credential to the database.

If the device does not have an SNMPv3 profile in the database, the Read Only credential for the default Profile in the database is assigned to the device. If no credential is assigned in the database, the credential entry remains a double hyphen ( -- ).

You can edit the Credential Name column for entries that list a valid credential. Click on the column to display a drop-down list that contains all SNMPv3 credentials from the NetSight database.

### Credential Information

This column shows the settings for the associated Credential Name. The source of the credential information is:

- The credential information settings in the NetSight database,
- The `snmptrapd.conf` file when an Engine ID matches an entry in the `snmptrapd.conf` file,
- Manually added entries using the **Add Entry** button.

### Modified

Indicates with an asterisk (\*) all table entries that do not have a matching entry in the **Text** area, either because it was just initialized when the application was launched or because it was added with the **Add Entry** button. When an entry that has been added or modified has a matching entry in the Text area or when a modified entry is entered into the **Text** area using the **Add to File** button, the Modified column is cleared for the entry.

### Text

This area is a text editor where you can make changes to the **snmptrapd.conf** file. It displays the entire, unfiltered contents of the **snmptrapd.conf** file. **Save** writes the file, using the complete text from this area.

### Status Line

As the devices information returns, the status line is updated and a progress bar indicates the percentage of devices that have been resolved. The status bar indicates the total number of devices to process, the number of devices whose Engine IDs have been received, the number of devices determined to be non-SNMPv3, and the number of devices that have not responded after all timeouts and retries have been exhausted.

### Remove Button

This button removes the currently selected row from the table.

### Add Entry Button

This button lets you add new entries to the Credential Table. The Credential Name column will display the Read Only credential for the default Profile. The Engine ID and Credential Name columns are editable for rows being added. The Credential Name drop-down list contains all of the SNMPv3 credentials available from the NetSight database. An Engine ID is only necessary for devices sending trap messages. It is not necessary for Informs. An error is reported when the Engine ID being entered matches another Engine ID in the table.

### Get EngineID Button

This button starts the process of requesting the Engine IDs again, in the same fashion as when the window is first opened, to update the table information. The process only attempts to contact devices whose IP address appear in the table.

### Add to File Button

Adds the row(s) currently selected in the Credential Table to the **Text** area.

### Save Button

Writes the changes you have made to the **snmptrapd.conf** file. The file is located on the server in <install directory>\NetSight\appdata directory.

---

## Related Information

For information on related tasks:

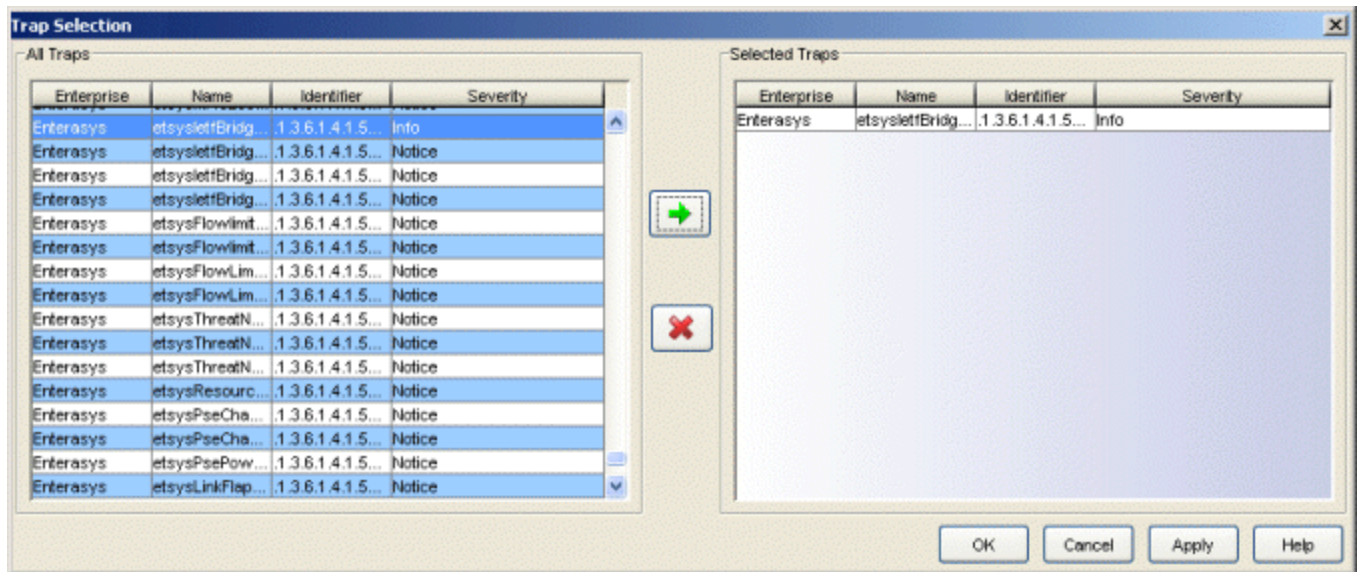
- [How to Configure the SNMP Trap Service](#)

For information on related concepts:

- [Traps and Informs](#)

## Trap Selection Window

This window lets you select specific traps that, when they occur, will trigger an alarm. The window is accessed from the **Edit Traps** button in the [Alarms Manager window](#).



### All Traps

This panel lists all of the Trap IDs available for the devices modeled in the NetSight database.

### Selected Traps

This panel lists traps that you've selected from the left panel. These are the traps that will trigger the selected action. When more than one trap is selected, the selected action will occur when any one of the selected traps occurs.



#### Add Trap

Adds one or more traps selected to the right panel.



#### Remove Trap

Removes one or more traps selected from the right panel.

## Related Information

For information on related windows:

- [Alarms Manager Window](#)

For information on related tasks:

- [How to Configure Alarms](#)



## VLAN Definitions

---

This window displays VLAN definition information for the associated VLAN model. In this window you can view all the existing VLAN definitions for the model, create new VLAN definitions, define and modify the settings for existing VLANs, and delete VLANs.

---

**NOTE:** Special care must be taken when configuring an X-Pedition Router. Refer to [Configuring VLANs on an X-Pedition Router](#) to review configuration caveats for this device.

---

To access this window, in the left panel, expand the VLAN Elements folder, then expand the desired VLAN model folder. Within the VLAN model folder, select the VLAN Definitions folder or a VLAN definition within it. The VLAN Definitions window appears in the right panel. Each VLAN model you create is pre-populated with a Default VLAN (VID 1). You can further define this VLAN, and/or you can create other VLANs.

The VLAN Definitions window consists of an upper panel and a lower panel. You can use the panel control buttons ▲▼ to hide or show the panels. The table in the upper panel lists the VLANs currently defined for the selected VLAN model, and gives you an overview of their properties. If you select a VLAN definition in the left panel or in the upper table, the selected VLAN's properties are displayed in the lower portion of the tab, and are available for editing. The lower panel is also used for creating new VLAN definitions.

Once you've defined or edited a VLAN definition, you can use the Device View of the [VLAN tab](#) in the Console's main window to enforce the VLAN properties on selected devices or to compare (verify) VLANs in a model against the VLAN settings on selected devices, and update a VLAN definition from the VLAN settings on a selected device.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

For more information, see [How to Work with VLAN Models](#).

VLAN Name	VLAN ID	Write To Device(s)	Dynamic Egress	IGMP Status	IGMP Version	Switch Query IP	Query Interval
Default VLAN	1	Yes	N/A	N/A	N/A	N/A	N/A

VLAN Name:  VLAN ID:

Write VLAN to Devices

Dynamic Egress:

X-Pedition Protocol Filter

Protocols

L4 Bridging - IP/IPX only

IP  IPX

Bridged-protocols  SNA

AppleTalk  IPv6

DEC

IGMP Parameters

IGMP Status:

IGMP Version:

Switch Query IP:

Query Interval:

Query Response:

Interface Robustness:

Last Member Query Interval:

## VLANs in VLAN Model

This table provides information on the VLANs currently associated with the VLAN model selected in the left panel. To view or change the properties of a VLAN, select it in this table or in the left panel. This displays the selected VLAN's properties in the lower part of the tab, and allows you to edit them. You can also delete VLANs from the model by selecting them in this table and clicking **Delete**. (The Default VLAN for a model cannot be deleted.)

### VLAN Name

Alphanumeric name associated with the VLAN ID.

### Write VLAN to Device(s)

When checked, the VLAN will be written to the device(s) when you [enforce](#).

### Dynamic Egress

When checked, the associated [dynamic egress](#) setting for the VLAN (Enable or Disable) will be written to the device(s) when you [enforce](#).

---

**NOTE:** Dynamic Egress is not supported on X-Pedition Routers

---

### X-Pedition Protocol Filter

When checked, the selected protocol filters will be applied in the device(s) when you [enforce](#):

- L4 Bridging - IP/IPX only
- IP
- Bridged-protocols
- AppleTalk
- DEC
- IPX
- SNA
- IPv6

### VLAN ID

([VID](#)) Unique number that identifies the VLAN.

### IGMP Status

When checked, the current [IGMP](#) (Internet Group Management Protocol) state (Enable or Disable) and the associated IGMP settings for the VLAN will be written to the device(s) when you [enforce](#):

- **N/A** - IGMP is not a part of the VLAN's definition.
- **Enable** - IGMP is a part of the VLAN's definition, and will be enabled.
- **Disable** - IGMP is a part of the VLAN's definition, but is currently disabled.

### IGMP Version

Indicates which version of [IGMP](#) will be utilized on the port (Version 1 or Version 2).

### Switch Query IP

The address of the IGMP Querier on the IP subnet to which this interface is attached.

### Query Interval

Interval (in seconds) between general IGMP queries sent by the device. Larger values cause queries to be sent less often. This value must be greater than the Query Response interval. Valid values: 1 through 300. For more information, see [IGMP](#).

**Query Response**

Maximum amount of time allowed for responses to general IGMP queries. Larger values result in less bursty traffic. This value must be less than the Query Interval. Valid values: 1 through 300. For more information, see [IGMP](#).

**Interface Robustness**

(Robustness Variable ) Indicates how susceptible the subnet is to lost packets. You might want to increase this value if you expect a subnet to be prone to losing packets. Valid values: 2 thru 32767. For more information, see [Interface Robustness](#).

**Last Member Query Interval**

Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds. See [IGMP](#) for more information.

## VLAN Definition

This section of the VLAN Definitions window displays the properties of the VLAN selected in the table in the upper panel or the left panel, and enables you to edit them. You can also create a new VLAN in this panel. To save a new VLAN or apply changes to an existing VLAN, click **Save**.

**VLAN Name**

Name of the VLAN selected in the upper table. If you create a [new](#) VLAN, this box is automatically filled with a new VLAN name (VLAN), which you can change. If you don't change it, the VLAN is named VLAN [n], where *n* is the value in the VLAN ID text box. Do not create a VLAN name that uses any letters with diacritical marks. Diacritical marked letters are not supported by SNMP.

**VLAN ID**

[VID](#) of the VLAN selected in the upper table. If you create a [new](#) VLAN, this box is automatically filled with the next available VID, which you can change if desired.

**Write VLAN to Device(s)**

Check this box if you want this VLAN's properties to be written to the device(s) when you [enforce](#) and compared to device settings when you [verify](#).

### Dynamic Egress

Check this box to make [dynamic egress](#) a factor for this VLAN. To enable dynamic egress, select Enable from the drop-down list.

## IGMP Parameters

This section of the VLAN Definitions window allows you to select and edit the [IGMP](#) (Internet Group Management Protocol) properties of the VLAN. The IGMP Status box must be checked in order to set the other IGMP parameters. If you turn on an IGMP element with its checkbox, it becomes a factor for the VLAN, and you can specify its appropriate setting using the text box or drop-down list for the element.

### IGMP Status

Check this box to make IGMP a part of this VLAN's definition. This box must be checked in order for the other IGMP parameters to be set. To enable IGMP, select Enable from the drop-down list.

### IGMP Version

Check this box to make the IGMP version on the port a factor for this VLAN. Select the version of IGMP that will be utilized from the drop-down list: Version 1 or Version 2.

### Switch Query IP

The address of the IGMP Querier on the IP subnet to which this interface is attached.

### Query Interval

Number of seconds allowed between general IGMP queries sent by the device. Check this box to make the query interval a factor for this VLAN. Enter the number of seconds in the text box, or use the up/down arrows to change the value. Larger values cause queries to be sent less often. This value must be greater than the Query Response interval. Valid values: 1 through 300. For more information, see [IGMP](#).

### Query Response

Maximum amount of time allowed for responses to general IGMP queries. Check this box to make the query response time a factor for this VLAN. Enter the number of seconds in the text box, or use the up/down arrows to change the value. Larger values result in less bursty traffic. This value must be less than the Query Interval. Valid values: 1 through 300. For more information, see [IGMP](#).

**Interface Robustness**

(Robustness Variable ) Indicates how susceptible the subnet is to lost packets. Check this box to make interface robustness a factor for this VLAN. Enter a value in the text box, or use the up/down arrows to change the value. You might want to increase this value if you expect a subnet to be lossy. Valid values: 2 thru 32767. For more information, see [Interface Robustness](#).

**Last Member Query Interval**

Maximum number of seconds allowed between group-specific query messages, including those sent in response to leave-group messages. Check this box to make the last member query interval a factor for this VLAN. Enter a value in the text box, or use the up/down arrows to change the value. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds. See [IGMP](#) for more information.

**New Button**

Creates a new VLAN. When you click this button, a new VLAN name appears in the lower left panel and the next available VID is automatically selected. The properties of the previously displayed VLAN are retained. To complete the new VLAN definition, change the VLAN name and/or VID if desired, edit the appropriate properties, and save.

**Save Button**

Saves the VLAN and its properties as part of the VLAN model.

**Delete Button**

Removes the currently selected VLAN from the VLAN model. An intermediate confirmation dialog box appears, giving you the opportunity to change your mind before the deletion occurs. Since the Default VLAN for a model cannot be deleted, if you select a Default VLAN as one of a several VLANs to be deleted, only the non-Default VLANs will be deleted.

---

**Related Information**

For information on related tasks:

- [How to Work with VLAN Models](#)

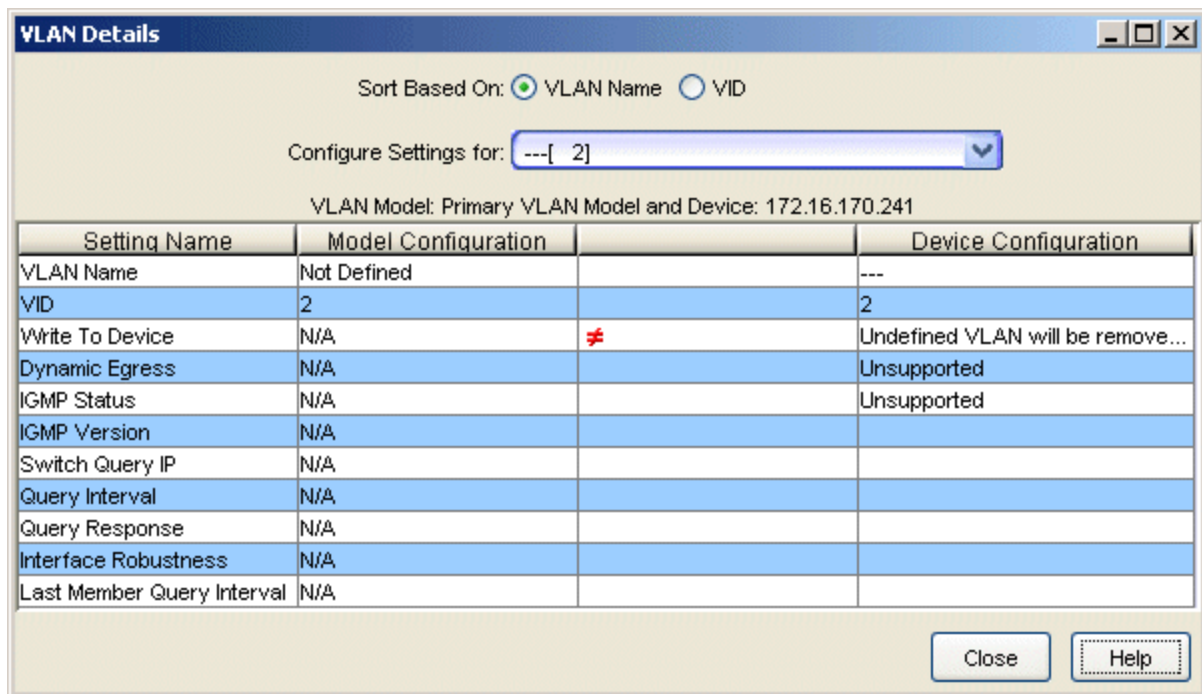
For information on related windows:

- [Port Template Definitions](#)

## VLAN Details Window

The VLAN Details window enables you to view the differences between a VLAN definition in a model and a device's VLAN configuration, prior to enforcing a VLAN definition or updating the definition from a device. To open this window, do a [Verify](#) in the Device view of the [VLAN Tab](#), then select the **VLAN Detail** button.

**NOTE:** Egress Lists on the device are not checked to see if the VLAN will be egressing any ports.



The screenshot shows the 'VLAN Details' window with the following configuration:

- Sort Based On:  VLAN Name  VID
- Configure Settings for: ---[ 2]
- VLAN Model: Primary VLAN Model and Device: 172.16.170.241

Setting Name	Model Configuration		Device Configuration
VLAN Name	Not Defined		---
VID	2		2
Write To Device	N/A	≠	Undefined VLAN will be remove...
Dynamic Egress	N/A		Unsupported
IGMP Status	N/A		Unsupported
IGMP Version	N/A		
Switch Query IP	N/A		
Query Interval	N/A		
Query Response	N/A		
Interface Robustness	N/A		
Last Member Query Interval	N/A		

Buttons: Close, Help

### Sort Based on:

Select how you want the list of VLANs in the **Configure Settings for** dropdown list sorted, by [VID](#) or [VLAN Name](#).

### Configure Settings for:

This dropdown list includes all the VLANs on the device selected in the [VLAN \(Device\)](#) tab, plus those in the VLAN model, sorted by VLAN Name or VLAN ID, depending on your **Sort Based on** selection. Depending on how the list is sorted, you can see whether the same VLAN name is being used for two VIDs, or vice versa. Select the VLAN whose configuration

settings you want to compare with the device settings in the VLAN Model and Device table.

## VLAN Model and Device Table

This table displays the differences in VLAN settings between the device selected in the [VLAN \(Device\)](#) tab and those in the VLAN model. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

### Setting Name

Lists the potential settings for a VLAN's definition. See [Properties Tab \(VLAN Definitions\)](#) for descriptions.

### Model Configuration

Indicates how the VLAN setting is configured in the VLAN definition. If the setting is not a part of the VLAN's definition, N/A is displayed. If the setting is part of the VLAN's definition, but is not currently enabled or defined, Not Defined is displayed.

### Difference

A red not-equals sign **≠** indicates that there is a difference in configuration between the definition in the VLAN model and the setting on the device. If the setting is not a part of the VLAN's definition, N/A is displayed. If the setting is part of the definition, but is not enabled or defined, Not Defined is displayed.

### Device Configuration

Indicates how the VLAN setting is configured on the device.

---

## Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

- [VLAN Tab \(Device\)](#)
- [VLAN Definitions View](#)
- [Port Template Definitions View](#)





## VLAN Egress Details Window

The VLAN Egress Details window lets you compare the egress state as defined in the selected port template with the current and static egress states of the port. To open this window, do a [Verify](#) in the Advanced Port view of the [VLAN Tab](#), then select the **Egress Details** button. A red not-equals sign **≠** in this table indicates that a difference has been detected between the setting in the port template and the setting on the port. If a non-enforceable difference is found, the **≠** is not displayed.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

VID	Model VLAN Name	Model Egress	Device Static Egress	Device Current Egress	Model PVID	Device PVID	VLAN
1	Default VLAN	Untagged	≠ No Egress	No Egress	Yes		Permane
2	VLAN 2	N/A	Not Defined	No Egress			Permane
3	VLAN3	N/A	Not Defined	No Egress			Permane
4	VLAN4	N/A	Not Defined	No Egress			Permane
5	VLAN7	N/A	Not Defined	No Egress			Permane
6	VLAN5	N/A	Not Defined	No Egress			Permane
7	VLAN6	N/A	Not Defined	No Egress			Permane
8		N/A	Not Defined	No Egress			Permane
9		N/A	Not Defined	No Egress			Permane
10		N/A	Not Defined	No Egress			Permane
11		N/A	Not Defined	No Egress			Permane
12		N/A	Not Defined	No Egress		≠ Yes	Permane
13		N/A	Not Defined	No Egress			Permane
14		N/A	Not Defined	No Egress			Permane
15		N/A	Not Defined	No Egress			Permane
78	VLAN	N/A	Not Defined	Unknown			---

## VLAN Egress Details Table

VID

[VLAN ID](#) of the listed VLAN.

Model VLAN Name

Lists the VLANs in the VLAN model.

## Model Egress

Egress state of the port as defined in the port template. Indicates whether frames forwarded out the port will be transmitted as tagged or untagged, or if no egress is allowed. Possible values are as follows:

- **No Egress** - No frames will be transmitted out the port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out the port.
- **Untagged** - Only untagged frames will be transmitted out the port.
- **No Change** - If the egress state is set to No Change, it won't be compared and a red not-equals sign **≠** will not appear.
- **N/A** - The port template's Set All Egress States checkbox is not checked; therefore, this setting is not applicable to the model.

See [Egress Rules](#) for more information.

## Device Static Egress

Static egress (forwarding) state of the port on the device. Indicates whether frames forwarded out the port will be transmitted as tagged or untagged, or if no egress is allowed. Static egress can be set using the Console VLAN tab. Possible values are as follows:

- **No Egress** - No frames will be transmitted out the port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out the port.
- **Untagged** - Only untagged frames will be transmitted out the port.
- **Not Defined** - A VLAN ID has been assigned to the port as a PVID, but this VLAN has not been created on the device (or in the Static VLAN Configuration table).

See [Egress Rules](#) for more information.

## Device Current Egress

Current egress state of the port on the device. Indicates whether frames forwarded out the port will be transmitted as tagged or untagged, or if no egress is allowed. The current egress state is determined by GVRP protocol (i.e. dynamic VLAN). Possible values are as follows:

- **No Egress** - No frames will be transmitted out the port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out the port.
- **Untagged** - Only untagged frames will be transmitted out the port.

- **Not Defined** - A VLAN ID has been assigned to the port as a PVID, but this VLAN has not been created on the device (or in the Static VLAN Configuration table).

See [Egress Rules](#) for more information.

#### Model PVID

Indicates whether or not the [Port VLAN ID](#) is set in the port template (Yes or No).

#### Device PVID

Indicates whether or not the [Port VLAN ID](#) is set on the port on the device (Yes or No).

#### VLAN Type

Displays the VLAN filtering/forwarding type. Possible values include:

- **Permanent** - The VLAN is active and will remain so after the next reset of the device.
- **Dynamic GVRP** - The VLAN is active and will remain so until removed by dynamic [GVRP](#).
- **Other** - The VLAN is active, but is not permanent or dynamic GVRP.
- **Create VLAN** - The VLAN is not on the device and needs to be created.

#### VLAN Status

Indicates the operational status of the VLAN. Possible values are: Enabled, Disabled, N/A.

#### Other VLAN Differences

Provides a description of other differences detected between the port template and the settings on the ports themselves. See [Description of Differences](#) for possible differences.

---

### Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

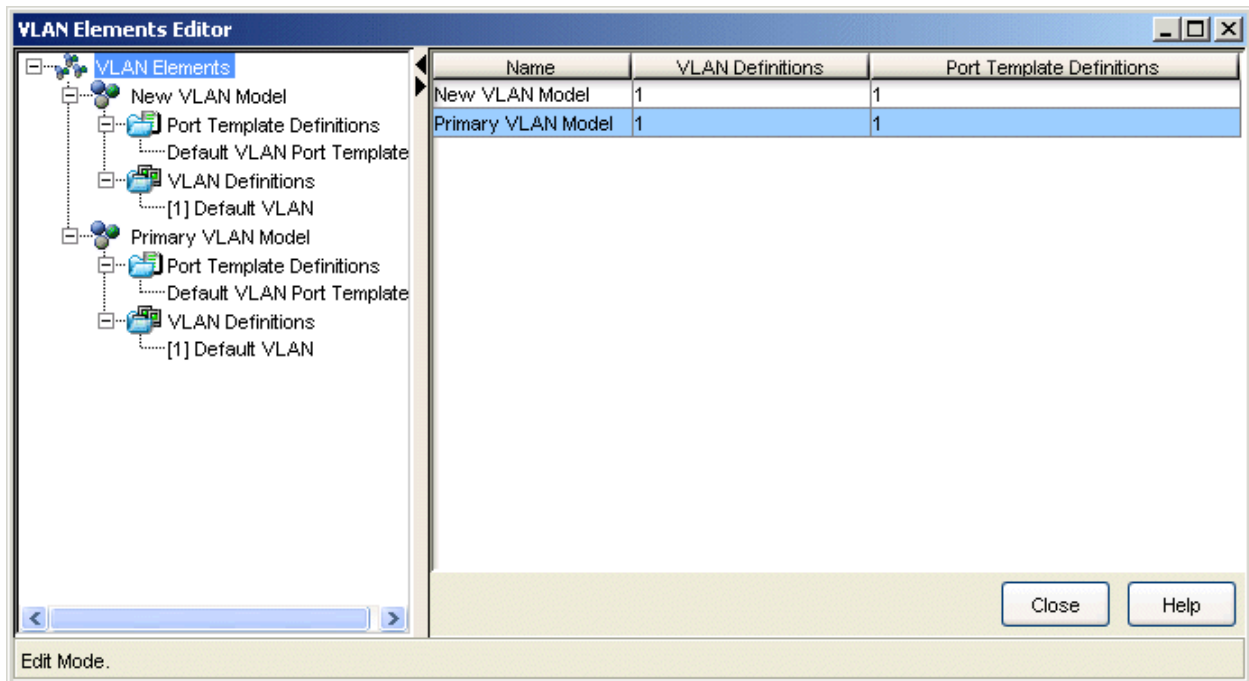
- [VLAN Tab \(Advanced Port\)](#)

## VLAN Elements Editor





The VLAN Elements Editor lets you view and configure the VLAN settings for your network. The left panel contains a tree hierarchy showing all of the VLANs that have been modeled in the Extreme Management Center (Management Center) database. The right panel lists the currently defined VLAN models and indicates the number of VLAN Definitions and Port Template Definitions that exist for each model.

When a Port Templates Definition is selected in the left panel, the [Port Template Definitions](#) view appears in the right panel. When a VLAN Definition is selected in the left panel, the [VLAN Definitions](#) view appears in the right panel. The Default VLAN Model and Default Port Templates allow you to establish default settings to help in configuring the VLANs on your network.

### *Sample VLAN Elements Editor window*



### Left Panel Icons

Icon	Definition	Icon	Definition
	VLAN Elements		VLAN Model
	Port Template Definition		VLAN Definition

## Right-click Menus

Several right-click menus are available from a right mouse click on icons in the left panel. The specific menu selections depends on the particular icon selected. The following table describes the available menu selections:

Menu Selection	Definition	Available From
<b>Add VLAN Model</b>	Adds a new VLAN Model under the VLAN folder.	VLAN Elements
<b>Delete VLAN Model</b>	Removes the selected VLAN model from the NetSight database.	VLAN Model
<b>Delete VLAN Port Template</b>	Removes the selected VLAN Port Template from the NetSight database.	VLAN Port Template
<b>Expand/Collapse</b>	Shows/hides sub-groups nested within the selected group.	All VLAN folders
<b>Rename</b>	Highlights the selected item name to allow typing a new name.	VLAN Port Template

## Name

Name of the VLAN model.

## VLAN Definitions

Number of VLAN definitions defined for the model.

## Port Template Definitions

Number of port templates defined for the model.

## Table Controls

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

**Related Information**

For information on related tasks:

- [How to Work with VLAN Models](#)

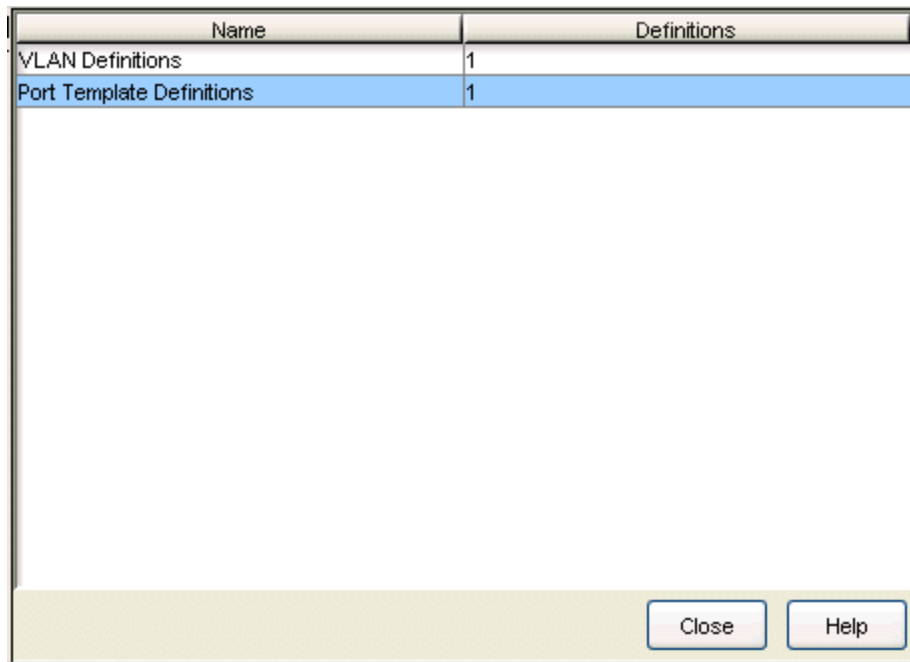
For information on related windows:

- [Port Template Definitions View](#)
- [VLAN Definitions View](#)

## VLAN Model

---

When a VLAN Model folder is selected in the left panel of the VLAN Elements Editor, the right panel lists the currently defined VLAN models and indicates the number of VLAN and port template definitions that exist for each model.



Name	Definitions
VLAN Definitions	1
Port Template Definitions	1

The screenshot shows a table with two columns: 'Name' and 'Definitions'. The first row is 'VLAN Definitions' with a value of '1'. The second row is 'Port Template Definitions' with a value of '1'. The second row is highlighted in blue. Below the table are two buttons: 'Close' and 'Help'.

### Name

Lists the types of definitions that comprise the VLAN model.

### Definitions

Number of definitions of this type that currently exist in the model.

### Table Controls

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

---

## Related Information

For information on related tasks:



- [How to Work with VLAN Models](#)

For information on related windows:

- [Port Template Definitions View](#)
- [VLAN Definitions View](#)

## VLAN Port Template Definitions View

---

This view displays port template definition information for the associated VLAN model. In this view you can view all the existing port templates for the model, create new port templates, define and modify the settings for existing port templates, and delete port templates.

To access this view, in the left panel, expand the VLAN Elements folder, then expand the desired VLAN model folder. Within the VLAN model folder, select the Port Template Definitions folder or a port template definition within it. The Port Template Definitions view appears in the right panel.

The view consists of an upper panel and a lower panel. You can use the panel control buttons ▲▼ to hide or show the panels. The table in the upper panel lists the port templates currently defined for the selected VLAN model, and gives you an overview of their properties. If you select a port template in the left panel or in the upper table, the selected port template's properties are displayed in the lower portion of the view, and are available for editing. The lower panel is also used for creating new port templates.

Once you've defined or edited a port template, you can use the [Basic Port](#) view of the **VLAN** tab in Console's main window to enforce templates or individual custom port settings to selected ports. You can also use the [Advanced Port](#) view of the **VLAN** tab in Console's main window to enforce the port template properties on selected ports or to compare (verify) port templates in a model against the port VLAN settings on selected devices, and update a port template from the port settings on a device.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

For more information, see [How to Work with VLAN Models](#).

VLAN Port Template for : New VLAN Model

Template Name	VLAN Name	PVID	Set PVID	PVID Egress State	Configure Egres...	Ingress Filtering	Default Port Prio.	Acceptable Fra...	GVRP
Default VLAN Port Te...	Default V...	1	N/A	Untagged	N/A	N/A	N/A	N/A	N/A

Template Name:

Set PVID:

PVID Egress State:

Ingress Filtering:

Default Port Priority:

Acceptable Frame Type:

GVRP State:

GARP Join Time:

GARP Leave Time:

GARP Leave All Time:

Configure Egress States  Show All VLANs

VID	VLAN Name	Model PVID	Egress State	Dynamic Egress
1	Default VLAN	Yes	Untagged	Disable

## VLAN Port Templates

This table provides information on the port templates currently associated with the VLAN model selected in the left panel. To view or change the settings for a particular port template, select the port template in this table or in the left panel. The selected port template's properties are displayed in the lower part of the tab, where they can be edited. You can also delete a template from the model by selecting it in this table and clicking **Delete**.

### Template Name

Name of the port template.

### VLAN Name

Name of the VLAN associated with the port template.

### PVID

([Port VLAN ID](#)) Numerical identifier of the VLAN associated with the port template.

**Set PVID**

Indicates whether or not the [Port VLAN ID](#) is set for this port template (Yes or No).

**PVID Egress State**

Indicates whether frames forwarded out the ports using this port template will be transmitted as tagged or untagged, or if no egress is allowed.

Possible values are as follows:

- **No Egress** - No frames will be transmitted out this port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out this port.
- **Untagged** - Only untagged frames will be transmitted out this port.
- **No Change** - Leave the egress state as it is.

See [Egress Rules](#) for more information.

**Configure Egress States**

Indicates whether or not the [Configure Egress States](#) box is checked for the port template. (Yes or No).

**Ingress Filtering**

Indicates whether or not [Ingress Filtering](#) is enabled or disabled on the ports using this port template.

---

**NOTE:** On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

---

**Default Port Priority**

Priority an incoming frame on the ports using this port template will receive, unless a priority is already assigned to it, or a priority classification rule exists. Possible values: 0 (lowest priority) through 7 (highest priority). For more information, see [Priority Classification](#).

**Acceptable Frame Type**

Indicates whether the ports using this port template will accept all frames (tagged and untagged) or only tagged frames. See the definition of [Acceptable Frame Types](#) in the lower left table for more information.

**GVRP State**

Indicates whether [GVRP](#) (GARP VLAN Registration Protocol) will be enabled or disabled on the ports using this port template.

### GARP Join Time

Frequency of messages issued by a device when a new port has been added to the VLAN. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

### GARP Leave Time

Frequency of messages issued by a device when a single port no longer belongs to the VLAN. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

### GARP Leave All Time

Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

## Port Template Properties

This section of the Port Template Definitions view displays the properties of the port template selected in the upper table or in the left panel, and enables you to edit them. You can also [create a new port template](#) in this panel. To save a new port template or apply changes to an existing port template, click **Save**.

### Template Name

Name of the port template. If you create a new port template, this box is automatically filled with a new port template name (e.g., New Port Template, New Port Template 1), which you can either change or leave as is.

### Set PVID

Check this box to set the [Port VLAN ID](#) for this port template, then select the desired PVID from the drop-down list.

### PVID Egress State

If Set PVID is checked, you can select the egress state for this port template from the drop-down list; otherwise, this option is not available. Changing the egress state for the selected PVID changes the VID in the VID table on the right, and vice-versa: right-clicking on the VLAN in the VID table and selecting an egress state changes the selection in the Port Template Properties area on the left.

- **No Egress** - No frames will be transmitted out this port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out this port.

- **Untagged** - Only untagged frames will be transmitted out this port.
- **No Change** - Leave the egress state as it is.

See [Egress Rules](#) for more information.

**Note:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

**Note:** On some devices, in order to properly configure the Egress State for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via Extreme Management Center Console.

### Ingress Filtering

Check this box to make [Ingress Filtering](#) a factor for this port template. To enable Ingress Filtering, select Enable from the drop-down list.

**Note:** On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

### Default Port Priority

Default priority for frames entering the port. A frame will receive this priority unless a priority is already assigned to it, or a priority classification rule exists. Check this box to make default ingress user priority a factor for this port template, then select the priority from the drop-down list, 0 (lowest priority) up to 7 (highest priority). For more information, see [Priority Classification](#).

### Acceptable Frame Type

Check this box to make acceptable frame type a factor for this port template, then select the frame type from the drop-down list. If a port is set to **Accept All**, both tagged and untagged frames can be processed. If it is set to **Accept Tagged Only** frames, only frames that contain a VLAN tag can be processed, and all untagged frames will be discarded. For more information, see [Frame Types](#).

**Note:** On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged Only, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged Only, then the port

automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.

### GVRP State

Check this box to make [GVRP](#) (GARP VLAN Registration Protocol) a factor for this port template. To disable GVRP, select Disable from the drop-down list. If the field is grayed out, the device does not support GVRP.

### GARP Join Time

Frequency of messages issued by a device when a new port has been added to the VLAN. Check this box to make GARP join time a factor for this port template, then enter the time, in milliseconds. Valid values are 1 through 1488800. The default value is 20. For more information, see [GARP Timers](#).

### GARP Leave Time

Frequency of messages issued by a device when a single port no longer belongs to the VLAN. Check this box to make GARP leave time a factor for this port template, then enter the time, in milliseconds. Valid values are 1 through 1488800. The default value is 60. For more information, see [GARP Timers](#).

### GARP Leave All Time

Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. Check this box to make GARP leave all time a factor for this port template, then enter the time, in milliseconds. Valid values are 1 through 1488800. The default value is 1000. For more information, see [GARP Timers](#).

## VID Table

This table displays the VLANs in the egress list for the selected port.

### Configure Egress States

Checking this box enables you to set egress state for the VIDs in this table via the right-click menu egress options.

### Show All VIDs

Select this box to show all the available VLAN IDs. Otherwise, only the VLANs currently defined in the selected VLAN model are shown.

### VID

([VID](#)) Unique number that identifies the VLAN.

### VLAN Name

Alphanumeric name associated with the VLAN ID.

### Model PVID

If Yes, indicates that the VID is being used as the [Port VLAN ID](#) in the port template selected on the left.

### Egress State

Egress state defined in the VLAN model. Indicates whether frames forwarded out the port will be transmitted as tagged or untagged, or if no egress is allowed. To set the egress state for a VID, make sure the [Configure Egress States](#) box is checked, then use the right-click menu for the VID.

Possible values are as follows:

- **No Change** - When the port template is enforced, this setting clears the egress list on the device for the VID. This is the default egress state for VIDs in the VID table.
- **No Egress** - No frames will be transmitted out the port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out the port.
- **Untagged** - Only untagged frames will be transmitted out the port. See [Egress Rules](#) for more information.

### Dynamic Egress

Indicates whether or not [dynamic egress](#) is enabled for the VLAN (Yes or No).

### IGMP

Indicates whether [IGMP](#) (Internet Group Management Protocol) is Enabled or Disabled on the ports associated with this VLAN.

### Make Q Trunk Button

Creates an 802.1Q trunk to provide a connection between switches that can carry traffic from several VLANs. VLAN traffic sent over an 802.1Q trunk is tagged to preserve the VLAN ID information so that packets are sent only to the ports associated with a VID of the incoming packet.

### New Button

Creates a new port template. When you click this button, a new port template name appears in the lower left panel, and the properties of the previously displayed port template are retained. To complete the new template, change the template name if desired, edit the appropriate properties, and save.



### Save Button

Saves the port template and its properties as part of the VLAN model.

### Delete Button

Removes the currently selected port template from the VLAN model. An intermediate confirmation dialog box appears, giving you the opportunity to change your mind before the deletion occurs.

---

## Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

- [VLAN Definitions View](#)

## VLAN Tab (Advanced Port)

---

The Advanced Port view of the VLAN tab enables you to do any or all of the following:

- compare ([verify](#)) port templates with device port settings
- [update](#) port templates with port VLAN settings
- write ([enforce](#)) port templates to ports

To access the Advanced Port view of the VLAN tab, select the device(s) or group(s) of interest in the left panel. Then select the VLAN tab in the right panel and select the Advanced Port radio button. The Advanced Port view of the VLAN tab consists of an [upper panel](#) and a [lower panel](#). Use the panel control buttons ▲▼ to control the display of the two panels.


Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

For more information, see [How to Work with VLAN Models](#).

The screenshot shows the VLAN configuration interface with the following components:

- Navigation Tabs:** Properties, Compass, VLAN (selected), Basic Policy, ACL Manager, Interface Summary.
- Device Selection:** Device, Basic Port, Advanced Port (selected), VLAN Model: Primary VLAN Model.
- Upper Panel Table:** A table with columns: Device, Type, Port, Name, Alias, VLAN Name, PVID, and Static PVID Egress. It lists 7 ports for device 12.22.77.133, all with PVID 1 and Untagged status.
- Port Template Table:** Shows settings for the 'Default VLAN Port Template'. Settings include PVID (N/A), PVID Egress (N/A), Ingress Filtering (N/A), Default Port Priority (N/A), Acceptable Frame Type (N/A), GVRP (N/A), GARP Join Time (N/A), GARP Leave Time (N/A), GARP Leave All Time (N/A), and Configure VLAN Egress (N/A).
- Actual Port Settings Table:** Shows settings for device 12.22.77.133 on port 6. Settings include PVID (1), PVID Egress (VID(1) on Device=Untagged), Ingress Filtering (Disabled), Default Port Priority (0), Acceptable Frame Type (Accept All), GVRP (Disabled), GARP Join Time (20), GARP Leave Time (60), GARP Leave All Time (1000), and Configure VLAN Egress (See Egress Details).
- Buttons:** Detail... and Help.

## Upper Panel

When you click **Retrieve** , the table in the upper panel displays port VLAN information for the devices selected in the left panel. It also indicates whether there are discrepancies between the VLAN settings on the ports and those in the port templates in the selected VLAN model. Ports on which differences are detected are marked in the table by a red not-equals sign  $\neq$ .

**NOTE:** If you change the device selection in the left panel, the data in this view continues to reflect the previously queried set of devices until you do another Retrieve, with one exception: if you enforce, then select a new set of devices and do a Retrieve, the devices to which you applied will be read instead of the current selection.

To compare the egress state as defined in a port template with the current and static egress states of a port, select the port in the upper table and the port template in the lower left table, and click the **Egress Details** button to open the [VLAN Egress Details](#) window.

## VLAN Model

Select the VLAN model whose port templates you want to view in the left table of the lower panel.

## Ports Table

This table provides port VLAN information for the ports on the device(s) selected in the left panel. After you [verify](#), a red not-equals sign **≠** indicates that there are differences between the VLAN port template and the port settings on the device(s). When you select a port on which a difference has been detected, the settings for the currently selected port template are displayed in the table, with green exclamation points **!** indicating which settings are different. Those settings marked **!** will be written to the device if you [enforce](#).

### Device

IP address of the device.

### Type

Device type (e.g. SSR).

### Port

The dot1d bridge port number.

### Name

The port name taken from the *ifName* MIB object.

### Alias

Shows the alias (ifAlias) for the interface.

### VLAN Name

Name of the VLAN associated with the port.

### PVID

([Port VLAN ID](#)) Represents the port's VLAN assignment. Possible values are 1 through 4094.

---

**NOTE:** On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

---

### PVID Egress State

Indicates whether frames forwarded out the ports using this port template will be transmitted as tagged or untagged, or if no egress is allowed.

Possible values are as follows:

- **No Egress** - No frames will be transmitted out this port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out this port.
- **Untagged** - Only untagged frames will be transmitted out this port.

- **Not Defined** - A VLAN ID has been assigned to the port as a PVID, but this VLAN has not been created on the device (or in the Static VLAN Configuration table).

See [Egress Rules](#) for more information.

---

**NOTE:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

---

### Port Owner

Indicates how the port's Egress State was configured: by management, by GVRP (GARP VLAN Registration Protocol), or by Dynamic Egress. Uses the Egress List.

### Port Operation Mode

Displays the port's operational mode. Uses the Egress List.

- **DTrunk** -- port's Egress State (for all VLANs) is Untagged and its Acceptable Frame Type setting is Accept All
- **QTrunk** -- port's Egress State (for all VLANs) is Tagged and its Acceptable Frame Types setting is Accept Tagged Only
- **Tagged** -- port's Egress State (for the VLAN designated as its PVID) is Tagged
- **Hybrid** -- port's Egress State (for the VLAN designated as its PVID) is Untagged, its Egress State (for the remaining VLANs) is No Egress, and its Acceptable Frame Types setting is Accept All
- **Untagged** -- port's Egress State (for the VLAN designated as its PVID) is Untagged
- **No Egress** -- port's Egress State (for the VLAN designated as its PVID) is No Egress
- **Unknown** -- port's operational mode is none of the above

---

**NOTE:** For the X-Pedition Router, port operational modes are:

- **Access Port** -- port's Acceptable Frame Types is Accept All, its Egress State is Untagged, and its PVID can be any VLAN.
  - **Trunk Port** -- port's Acceptable Frame Types is Accept Tagged Only, its Egress State is Tagged, and its PVID is the Default VLAN.
-

### Ingress Filtering

Indicates whether or not [ingress filtering](#) is enabled or disabled on the ports using this port template.

---

**NOTE:** On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

---

### Default Port Priority

Priority an incoming frame on the ports using this template will receive, unless a priority is already assigned to it, or a priority classification rule exists. Possible values: 0 (lowest priority) through 7 (highest priority). For more information, see [Priority Classification](#).

### Acceptable Frame Type

Indicates whether the ports using this port template will accept all frames (tagged and untagged) or only tagged frames. See the definition of [Acceptable Frame Type](#) in the Properties Tab (Port) help topic for more information.

### GVRP

Indicates whether [GVRP](#) (GARP VLAN Registration Protocol) will be enabled or disabled on the ports using this port template.

### GARP Join Time

Frequency of messages issued by a device when a new port has been added to the VLAN. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

### GARP Leave Time

Frequency of messages issued by a device when a single port no longer belongs to the VLAN. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

### GARP Leave All Time

Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. Possible values are 1 through 2147483647 milliseconds. For more information, see [GARP Timers](#).

## Lower Panel

The left table in the lower panel lists the settings for the selected port template, and the right table lists the port VLAN settings on the port selected in the upper table. If desired, you can update the port template settings with the actual port

settings on the device using the **Update (Merge)** button .

To compare the egress state as defined in a port template with the current and static egress states of a port, select the port in the upper table and the port template in the lower left table, and click the **Egress Details** button to open the [VLAN Egress Details](#) window.

## Port Template Table

This table displays the settings in the selected port template.

### Port Template

After selecting a [VLAN Model](#), select a port template to view in the VLAN Port Template table.

### Settings

Lists the port template settings in the VLAN model. For definitions, see [Port Template Definitions](#) view.

### Values

Indicates how this setting is configured in the VLAN definition.

## Actual Port Settings on Device

This table shows the actual settings on the port selected in the upper table. A red not-equals sign **≠** indicates that there are differences between the VLAN port template and the port settings on the device(s).

### Settings

Lists the port settings on the device. For definitions, see [Port Template Definitions](#) view.

### Values

Indicates how this setting is currently configured on the port.





### VLAN Element Editor Button

Opens the [VLAN Element Editor](#) window where you can modify existing VLAN models or create new ones.







### Enforce Button

Writes the port template selected in the VLAN Port Template table to the port(s) selected in the upper table. If you select a line with a difference **≠** in the upper table, the port template settings are displayed, with a green

exclamation point  indicating that the setting is different and will be written to the device when you enforce. A VLAN's [Write VLAN to Devices](#) property must be set in order for an associated port template to be enforced. A red  appears if the enforcing of a particular setting fails.

### Start/Stop Verify (Retrieve) Button

Compares the VLAN model's port template settings with the port VLAN settings on the selected device(s). Only those port templates associated with VLANs whose [Write VLAN to Devices](#) property is set are verified.

When you initiate the verification process, this button changes to **Stop** , and you can stop the verification at any time. If there are no VLAN models against which to compare the device port VLAN settings, this button is grayed out. If a difference is detected, a red not-equals sign  is displayed on the appropriate line in the upper table. If you select  a line in the table, the port template settings are displayed. A green exclamation point  on that line indicates that the setting is different from the current setting on the port and will be written to the device if you enforce.

### Update (Merge) Button

[Updates](#) the port template settings in the lower panel left table with the [device port settings selected in the right table](#).

**CAUTION:** This operation cannot be undone.

---

### Details Button

Opens the [VLAN Egress Details](#) window.

---

## Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)


For information on related windows:

- [VLAN Egress Details Window](#)



## VLAN Tab (Basic Port)

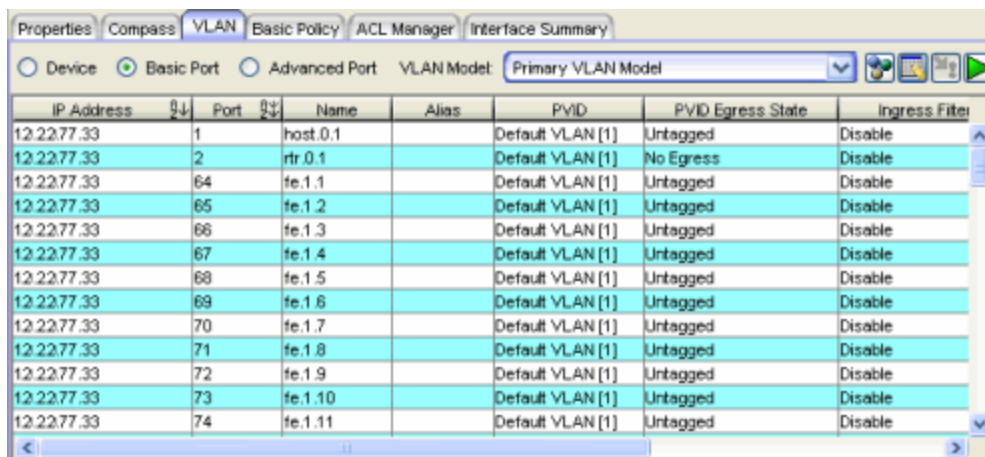
The Basic Port view of the VLAN tab enables you to view the port VLAN settings on selected device(s) in table form. You can select a VLAN port template to [enforce](#) to some or all of the ports in the table, or you can [edit](#) port data and enforce the individual changes.

To access the Basic Port view of the VLAN tab, select the device(s) of interest in the left panel, then select the VLAN tab in the right panel and select the Basic Port radio button. To populate the table, click **Retrieve** .

To perform a more detailed analysis of the differences between a [port template](#) and the port VLAN settings on the selected device(s), use the [Advanced Port](#) view of the VLAN tab.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic. In addition, you can right-click on a port and open the [Port Monitor](#) (Port Tools > Port Monitor).

For more information, see [How to Work with VLAN Models](#).



The screenshot shows a software interface with tabs for Properties, Compass, VLAN, Basic Policy, ACL Manager, and Interface Summary. The 'VLAN' tab is active, and the 'Basic Port' radio button is selected. A dropdown menu shows 'Primary VLAN Model'. Below is a table with columns: IP Address, Port, Name, Alias, PVID, PVID Egress State, and Ingress Filter. The table contains 14 rows of data for various ports on a device with IP 12.22.77.33.

IP Address	Port	Name	Alias	PVID	PVID Egress State	Ingress Filter
12.22.77.33	1	host.0.1		Default VLAN [1]	Untagged	Disable
12.22.77.33	2	rtr.0.1		Default VLAN [1]	No Egress	Disable
12.22.77.33	64	fe.1.1		Default VLAN [1]	Untagged	Disable
12.22.77.33	65	fe.1.2		Default VLAN [1]	Untagged	Disable
12.22.77.33	66	fe.1.3		Default VLAN [1]	Untagged	Disable
12.22.77.33	67	fe.1.4		Default VLAN [1]	Untagged	Disable
12.22.77.33	68	fe.1.5		Default VLAN [1]	Untagged	Disable
12.22.77.33	69	fe.1.6		Default VLAN [1]	Untagged	Disable
12.22.77.33	70	fe.1.7		Default VLAN [1]	Untagged	Disable
12.22.77.33	71	fe.1.8		Default VLAN [1]	Untagged	Disable
12.22.77.33	72	fe.1.9		Default VLAN [1]	Untagged	Disable
12.22.77.33	73	fe.1.10		Default VLAN [1]	Untagged	Disable
12.22.77.33	74	fe.1.11		Default VLAN [1]	Untagged	Disable

### VLAN Model

Select the VLAN model containing the port template you want to enforce here.



**VLAN Editor Button**

Opens the [VLAN Element Editor](#) window where you can modify existing VLAN models or create new ones.



**Show/Hide Table Editor Button**

Toggles the [Custom](#) edit area at the bottom of the table open and closed. If selected after making changes in the table editor, this button cancels any changes you made and restores the original values in the table.


**Enforce Button**

Writes the changes made using the [Custom](#) selection to ports in the table. A green exclamation point  in the table indicates that the setting will be written to the port when you enforce. A red  appears if the enforcing of a particular setting fails.

**Start/Stop Retrieve Button**

Retrieves port VLAN information from the device(s) selected in the left panel, or stops the retrieval. To start the retrieval, click . You can stop the retrieval before it is completed by clicking  at any time.

## Ports Table

This table displays VLAN information about the individual ports on the device(s) selected in the left panel. To populate this table, make a selection in the left panel and click .

**IP Address**

IP address of the device.

**Port**

The dot1d bridge port number.

**Name**

The port name taken from the *ifName* MIB object.

**Alias**

Shows the alias (ifAlias) for the interface.

**PVID**

([Port VLAN ID](#)) Represents the port's VLAN assignment. Possible values are 1 through 4094.

**NOTES:** On an X-Pedition Router:

1. You cannot assign a PVID to a port if the VLAN does not exist on the device. You must first **Enforce** the VLANs from the VLAN tab Device view to synchronize VLAN information between Console and the device.
  2. You cannot assign a PVID to a port that has an interface assigned to it.
  3. You cannot overwrite the PVID on a port used by a *System Static* VLAN (e.g., SYS\_L2\_InterfaceName).
  4. You can change the PVID on an access port (port with the Acceptable Frame Type set to Accept All) under the following conditions:
    - The port must be in the VLANs egress list.
    - The VLAN protocol for the access port is not being used by another VLANs protocol.
- 

### PVID Egress State

Indicates whether frames forwarded out the port will be transmitted as tagged or untagged, or if no egress is allowed. Possible values are as follows:

- **No Egress** - No frames will be transmitted out this port. They will be discarded.
- **Tagged** - Only tagged frames will be transmitted out this port.
- **Untagged** - Only untagged frames will be transmitted out this port.
- **Not Defined** - A VLAN ID has been assigned to the port as a PVID, but this VLAN has not been created on the device (or in the Static VLAN Configuration table).

See [Egress Rules](#) for more information.

---

- NOTES:**
1. On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.
  2. On some devices, in order to properly configure the Egress State for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via NetSight Console.
- 

### Ingress Filtering

Indicates whether or not [ingress filtering](#) is enabled on this port (true or false).

---

**NOTE:** On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

---



### Default Port Priority

The priority an incoming frame on this port will receive (unless a priority is already assigned to it or a priority classification rule exists). Possible values: 0 (lowest priority) through 7 (highest priority). For more information, see [Priority Classification](#).

### Acceptable Frame Type

Indicates whether this port will admit all frames (tagged and untagged) or only tagged frames. See the definition of [Acceptable Frame Type](#) on the port template Properties Tab for more information.

## Custom/Port Template

This area at the bottom of the table opens when you click the Show/Hide Table Editor button . It enables you to change individual port settings. You can either edit the existing port setting, or use the settings from a port template selected from the **Custom** drop-down list. Settings that will be changed when you [enforce](#) are marked with a green exclamation point  after editing a column. For more information, see [Editing Port VLAN Settings](#).

---

**NOTES:** To cancel changes and restore the original values, hide the Table Editor before enforcing the values in the table.

GVRP, GARP Join Time, GARP Leave Time, GARP Leave All Time, and Configure Egress States are not set in the Basic Port view. Use the Advanced Port View to set these values.

---

## Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

- [Properties Tab \(Port Template\)](#)
- [VLAN Tab \(Advanced Port\)](#)

## VLAN Tab (Device)

---

The Device view of the VLAN tab enables you to do any or all of the following:

- compare ([verify](#)) model VLAN definitions with VLAN settings on devices
- [update](#) model VLAN definitions with VLAN settings from devices
- write ([enforce](#)) model VLAN definitions to devices

To access the Device view of the VLAN tab, select the device(s) or group(s) of interest in the left panel. Then select the VLAN tab in the right panel and confirm that the Device radio button is selected. The Device view of this tab consists of an [upper panel](#) and a [lower panel](#). Use the panel control buttons ▲▼ to control the display of the two panels.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see the Table Tools Help topic.

For more information, see [How to Work with VLAN Models](#).

The screenshot shows the 'VLAN' tab in a network management interface. At the top, there are tabs for 'Properties', 'Map', 'VLAN', 'Compass', and 'Interface Summary'. Below these are radio buttons for 'Device' (selected), 'Basic Port', and 'Advanced Port', and a dropdown for 'VLAN Model' set to 'Primary VLAN Model'. A green play button icon is visible.

The main table displays the following data:

Device	Type	Status	Number of VLANs	VLANs With Conflicts	VLANs v
10.20.150.119	SmartSwitch 600...	Up	0	Unknown	Unknowr
10.20.150.114	SmartSwitch 600...	Up	0	Unknown	Unknowr
10.20.150.112	Matrix E7 6G306-06	Up	1	7	0
10.20.150.129	Vertical Horizon V...	Up	1	7	7
10.20.150.128	Vertical Horizon V...	Up	51	7	1
10.20.150.130	Vertical Horizon V...	Up	1	7	7
10.20.150.127	Vertical Horizon V...	Up	6	6	3
10.20.150.100	SmartSwitch 200...	Up	2	7	0
10.20.150.125	Vertical Horizon V...	Up	6	6	3
10.20.150.2	X-Pedition SSR 80	Up	9	7	1

Below the table are two comparison tables:

**VLAN Definitions for Model: Primary VLAN Model**

VLAN Name	VLAN ID ^	Write To De...	Dy
Default VLAN	1	Yes	N/
VLAN 2	2	Yes	N/
VLAN3	3	Yes	N/
VLAN4	4	Yes	N/

**VLAN Definitions for Device: 10.20.150.125**

VLAN Name	VID ^	Description of
DEFAULT	1	None
≠ VLAN2	2	VLAN Name mis
VLAN3	3	None
≠ purple	4	VLAN Name mis

Buttons at the bottom include 'VLAN Details...' and 'Help'.

## Upper Panel

The table in the upper panel provides VLAN information about the device(s) selected in the left panel. You can compare the current VLAN settings on the selected device(s) with the VLAN definitions in the selected VLAN model by clicking **Start Verify (Retrieve)** . Devices on which differences are detected are marked in the table by a red not-equals sign **≠**.

### View Selection

Select the Device radio button to see the Device view of the VLAN tab.

### VLAN Model

Select the VLAN model whose VLAN definitions you want to display in the left table of the lower panel.

## Device VLANs Table

This table provides VLAN information for the device(s) selected in the left panel. A red not-equals sign **≠** indicates that there are differences between the VLAN definitions in the model and the VLAN settings on the device(s).

---

**NOTE:** When you create multiple VLAN models, consult the **Max VLANs Supported** and **Max VLAN ID** values in this table, and create your VLANs based on the limitations of the device you are configuring. This will help you to avoid enforcing problems arising from conflicts between the maximums in a template and the maximums supported on a device.

---

### Device

IP address of the device.

### Type

Device type (e.g. SSR, X-Pedition, SmartSwitch, etc.).

### Status

This column indicates whether or not the device is up or down. Possible values include: Up, Down or Error returned:Timed out.

### Number of VLANs

Numerical count of the VLANs on the device.

### VLANs With Conflicts

Total number of VLANs on the devices that do not match the VLAN settings in the model.

### VLANs With Unsupported Differences

Total number of VLANs on the device(s) that do not support dynamic egress, IGMP and X-Pedition Protocol when checked in the model.

### VLANs Not In Model

Number of VLANs that are on the device(s) but not in the model.

### VLANs Not In Device

Number of VLANs that are in the model but not on the device(s).

### Max Supported VLANs

Maximum number of IEEE 802.1Q VLANs that this device supports. Consult this value when creating VLANs, to avoid enforcing problems arising from conflicts between the number of VLANs in a template and the number of VLANs supported on a device.

**Max VLAN IDs**

Maximum IEEE 802.1Q VLAN IDs that this device supports. Consult this value when creating VLANs, to avoid enforcing problems arising from conflicts between the maximum VID in a template and the maximum VID supported on a device.

**Traffic Classes Enabled**

Indicates whether or not [weighted priority](#) is enabled on the device. Possible values are: Enabled, Disabled, Unknown.

**GVRP Status**

Indicates whether [GVRP](#) (GARP VLAN Registration Protocol) will be enabled or disabled on the ports using this VLAN.

**IGMP New Default State**

Indicates the [IGMP](#) (Internet Group Management Protocol) state of the device:

- **Enabled** - IGMP is enabled.
- **Disabled** - IGMP is disabled.
- **Unsupported** - IGMP is not supported on the device.
- **Unknown** - The IGMP state of the device is not known.

**Extended Multicast Filtering Services**

Indicates whether extended multicast filtering services are implemented. Devices that implement this functionality can perform filtering of individual multicast addresses controlled by GMRP (GARP Multicast Registration Protocol). GMRP is a protocol used to register multicast addresses on ports to control flooding of multicast frames. Possible values include: Yes, No, Unknown.

**Traffic Classes**

Indicates whether or not [weighted priority](#) is available on this device. Possible values include: Yes, No, Unknown.

**Static Entry Individual Port**

Indicates whether or not static entry individual port is implemented. If Yes, ports from which frames must be received for filtering information to apply may be specified. Possible values include: Yes, No, Unknown

**VLAN Learning**

Displays the filtering database modes of operation implemented by the device:



- IVL -- Independent VLAN Learning
- SVL -- Shared VLAN Learning
- IVL/SVL -- Both Independent and Shared VLAN Learning
- Unknown -- Filtering database mode unknown

See [VLAN learning](#) for more information.

### Configurable PVID Tagging

Indicates whether or not configurable PVID tagging is implemented.

Devices that implement this functionality have the ability to override the default PVID setting and the egress state (Tagged or Untagged) on each port. Possible values include: Yes, No, Unknown.

### Local VLAN Capable

Indicates whether or not the device can support multiple local bridges, outside of the scope of 802.1Q defined VLANs. Possible values include: Yes, No, Unknown.

## Lower Panel

The left table in this panel shows the VLAN definitions in the VLAN model selected at the top, and the right table shows the VLAN settings on the device selected in the upper table. You can [update](#) the VLAN model with selected device settings, if desired.

**Note:** Egress Lists on the device are not checked to see if the VLAN will be egressing any ports.

## VLAN Definitions for Model

This table displays the VLANs defined for the VLAN model selected at the top of the tab.

### VLAN Name

Name of the VLAN.

### VLAN ID

[VLAN ID](#)) Unique numerical identifier of the VLAN.

### Write to Device(s)

Indicates whether or not the VLAN will be written to the device(s) when you [enforce](#), or compared to the actual VLANs on the device(s) when you [verify](#) (Yes or No).

### Dynamic Egress

Indicates whether or not [dynamic egress](#) is enabled for the VLAN (Yes or No).

### IGMP Status

Indicates whether [IGMP](#) (Internet Group Management Protocol) is a factor in this VLAN's definition, and if so, if it is to be enabled or disabled:

- **N/A** - IGMP is not a part of the VLAN's definition.
- **Enable** - IGMP is a part of the VLAN's definition, and is enabled.
- **Disable** - IGMP is a part of the VLAN's definition, but is currently disabled.

### IGMP Version

For VLANs using [IGMP](#), the version of IGMP that will be utilized on ports associated with the VLAN (Version 1, Version 2).

### Switch Query IP

The address of the IGMP Querier on the IP subnet to which this interface is attached.

### Query Interval

Interval (in seconds) between general IGMP queries sent by the device. Larger values cause queries to be sent less often. This value must be greater than the Query Response interval. Valid values: 1 through 300. For more information, see [IGMP](#).

### Query Response

Maximum amount of time allowed for responses to general IGMP queries. Larger values result in less bursty traffic. This value must be less than the Query Interval. Valid values: 1 through 300. For more information, see [IGMP](#).

### Interface Robustness

(Robustness Variable) Indicates how susceptible the subnet is to lost packets. A higher value may indicate that the subnet is particularly susceptible to losses. For more information, see [Interface Robustness](#).

### Last Member Query Interval

Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. Lower intervals reduce the amount of time it takes the device to detect the loss of the last member of a group. See [IGMP](#) for more information.

## VLANs Definitions for Device

This table shows the VLANs currently defined on the device selected in the upper table. A red not-equals sign **≠** indicates that there are differences between the VLAN model definition and the VLAN setting on the device.

### Description of Differences

Description of the discrepancies detected between the VLAN definitions in the model and the VLAN settings on the devices. Possible differences include:

- Dynamic Egress is Disabled on Device
- Dynamic Egress is Enabled on Device
- Dynamic Egress is not supported on Device
- IGMP Interface Robustness on device is 100
- IGMP Last Member Query Interval on device is 100
- IGMP not active for VID <number>
- IGMP not enabled on Device
- IGMP not supported on Device
- IGMP Query Interval on device is 100
- IGMP Query Response on device is 100
- IGMP Version on Device is <version>
- VLAN is not in VLAN Model
- VLAN is not on Device
- VLAN Name mismatch for VID <number>
- VLAN Not fully defined on Device

### VLAN Name

Name of the VLAN.

### VID

Numerical identifier of the VLAN ([VLAN ID](#)).

### Type

Displays the VLAN filtering/forwarding type. Possible values include:

- **Permanent** - The VLAN is active and will remain so after the next reset of the device.

- **GVRP** - The VLAN is active and will remain so until removed by dynamic [GVRP](#).
- **Other** - The VLAN is active, but is not permanent or dynamic GVRP.
- **Create VLAN** - The VLAN is not on the device and needs to be created.

### Status

Indicates whether the VLAN is enabled on the device. Possible values include: Enabled, Disabled, Other, N/A.

### Dynamic Egress

Indicates whether or not [dynamic egress](#) is enabled for the VLAN (Yes or No).

### IGMP Status

Indicates the [IGMP](#) (Internet Group Management Protocol) status of the VLAN:

- **Unsupported** - IGMP is not supported on the device.
- **Not Defined** - IGMP is supported on the device, but is not a part of the VLAN's definition.
- **Enabled** - IGMP is supported on the device, is a part of the VLAN's definition, and is enabled.
- **Disabled** - IGMP is supported on the device, is a part of the VLAN's definition, and is disabled.

For the definitions of the remaining columns in this table, see [VLAN Definitions for Model](#).



### VLAN Element Editor Button

Opens the [VLAN Element Editor](#) window where you can modify existing VLAN models or create new ones.



### Enforce Button

Writes the VLAN selected in the VLAN Definitions for Model table to the device(s). The VLAN's [Write VLAN to Devices](#) property must be set in order for its definitions to be enforced. To avoid unpredictable results, allow the enforce to complete before selecting another tab or device.

---

**NOTE:** On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS\_L3\_Interface Name). However, you can [update](#) a VLAN model definition with the System Static VLAN definition from the router.

---

 **Start/Stop Verify (Retrieve) Button**

Compares the selected model's VLAN definitions with the VLAN settings on the selected device(s), and displays the discrepancies in the upper table. Only those VLANs whose [Write VLAN to Devices](#) property is set are verified. When you initiate the verification process, this button changes to **Stop**, and you can stop the verification at any time. If there are no VLAN models against which to compare the device VLAN settings, this button is grayed out. If a difference is detected, a red not-equals sign **≠** is displayed in front of the appropriate line in the table.

 **Update (Merge) Button**

[Updates](#) the selected VLAN definition in the VLAN Definitions for Model table with the device VLAN settings selected in the right table. To avoid unpredictable results, allow the merge to complete before selecting another tab or device.

**CAUTION:** This operation cannot be undone.

---

**NOTE:** Certain devices that allow the creation of VLANs without VLAN names may create VLANs with blank names in the model. You can [rename](#) these if you like, or leave them blank. Either way, these VLANs and their properties (modified or not) will be saved when you click **Save**.

---

### VLAN Details

Opens the [VLAN Details](#) window.

---

### Related Information

For information on related tasks:

- [How to Work with VLAN Models](#)

For information on related windows:

- [VLAN Details Window](#)

# Reference Information

---

The **Reference Information** help section contains reference information and procedures for NetSight.

## Compass SNMP MIBs Descriptions

---

This topic provides a brief description of the MIBs and Tables that can be chosen as Compass Search Options when setting [Compass options](#).

### ipNetToMedia

IP Address Translation table used for mapping from IP addresses to physical addresses. This table is read whenever an entry is found by **IP Route** or **IP CIDR Route** searches, regardless whether the **IPNetToMedia** is checked. Checking the IPNetToMedia checkbox only affects whether or not the entire IPNetToMedia table is read.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

### 802.1x Authentication (PAE)

Port Access Entity module for managing IEEE 802.1X.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### MAC Locking

Provides configuration and status objects pertaining to per port MAC Locking.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### Enterasys IGMP

Extends the Standard IGMP MIB for configuration of IGMP on Enterasys devices.

Check this MIB to find other occurrences of an IP address or MAC address

within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **RMON addressMap**

MAC address to network address bindings discovered by the probe and what interface they were last seen on.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **Dot1dTpFdb**

This table contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

Check this MIB to resolve MAC addresses to a port.

### **Enterasys 802.1x Ext.**

Supplements/used in connection with the standard IEEE 802.1x MIB. It provides a convenient way to retrieve authentication status for Supplicants living on shared-media ports that use station-based access control. (Here, a MAC address is a much more natural table index than a port or interface number.)

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **Node/Alias (ctAlias)**

This MIB defines objects that can be used to discover end systems per port, and to map end system addresses to the layer 2 address of the port.

Check this MIB to resolve IP addresses to MAC addresses when the devices in your network support the Node/Alias (ctAlias) MIB.

### **IGMP Standard**

MIB module for IGMP Management, it contains an IGMP Interface Table, having one row for each interface on which IGMP is enabled, and an IGMP



Cache Table with one row for each IP multicast group for which there are members on a particular interface.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **IP Route**

An entity's IP Routing table. This selection provides the ability to resolve IP addresses to MAC addresses.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

### **Dot1qTpFdb**

A table that contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

### **PWA (Enterasys Port Web Authentication)**

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **MAC Authentication**

Used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **RMON host table**

Contains entries for each address discovered on a particular interface. Each entry contains statistical data about that host. This table is indexed by the

MAC address of the host, through which a random access may be achieved.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

### **IP CIDR Route**

The IP CIDR Route Table obsoletes and replaces the ipRoute Table current in MIB-I and MIB-II and the IP Forwarding Table. It adds knowledge of the autonomous system of the next hop, multiple next hops, and policy routing, and Classless Inter-Domain Routing.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

### **Dot1q VLAN Static**

A table containing static configuration information for each VLAN configured into the device by (local or network) management. All entries are permanent and will be restored after the device is reset.

### **Dot1q VLAN Current**

A table containing current configuration information for each VLAN currently configured into the device by (local or network) management, or dynamically created as a result of GVRP requests received.

### **Enterasys Multiple Authentication**

This MIB is used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication. Check this MIB to find ports that allow authentication of multiple users on a port.

### **Enterasys Convergence End Point**

This MIB contains information about devices that support End Point Convergence. Check this MIB to find IP addresses running applications (e.g. Voice over IP) using Endpoint Convergence.

## How to Add Trap Definitions

---

You can add trap definitions that can trigger Alarms, which can be configured to take a specific action, such as running a program or automatically sending e-mail messages. Trap definitions are added manually, using a text editor.

---

**CAUTION:** You should always save a copy of the trap definition file prior to editing and testing your new definitions.

---

To define a new trap:

1. Using your favorite text editor, open the `trapd.conf` file in the `<install directory>\NetSight\services` directory. This is a text file that can be edited to modify the severity levels for particular traps or add trap definitions to support devices.
  2. Add Event Definition using the format described in the `trapd.conf` file.
  3. Save the file.
- 

### Related Information

For information on related windows:

- [Main Window](#)
- [Alarms Manager Window](#)
- [Trap Selection Window](#)

## NetSight Data Synchronization

---

NetSight Application Data is stored in the <install\_directory>\NetSight\appdata directory on the NetSight Server. The directory contains data and configuration files used by the NetSight Server and shared between all clients. It also contains synchronized resources that are automatically distributed to each client. Having synchronized resources in one directory on the server allows for a single place to add and edit files without requiring changes to be made on each individual client.

User Data is stored in a NetSight folder in the user's home directory. This directory contains user-specific options and settings as well as synchronized resources from the NetSight Server. If this directory is removed, the user defaults back to a common set of options and settings.

NetSight uses the Data Synchronization Manager as a mechanism to keep client resources in sync with server resources. When files are updated on the server, the Data Synchronization Manager automatically distributes the resources to each client. Each resource to be distributed is zipped up and a checksum is calculated. If the resource does not exist on the client or if the checksum of the resource is different on the client, the client resource is backed up and the updated resource from the server is transferred to the client and extracted.

NetSight stores the following data as synchronized resources on the NetSight Server:

<b>Resource</b>	<b>Server Location</b>	<b>Client Location</b>
MIBs	appdata\System\mibs	User.home\NetSight\System\mibs
FlexViews	appdata\System\FlexViews	User.home\NetSight\System\FlexViews
Device Types	appdata\System\deviceTypes	User.home\NetSight\System\deviceTypes
Images	appdata\System\Images	User.home\NetSight\System\Images
Shared	appdata\System\Shared	User.home\NetSight\System\Shared

## Extreme Management Center Log Files

---

Extreme Management Center log files collect alarm, event, and trap information for Extreme Management Center Console and Extreme Management Center applications, and the devices on your network. The log files are displayed in the Extreme Management Center Event View (in the Console main window). By default, there is a Console log file and a log file for each application, as well as a Traps log and a Syslog log. In addition, the Server Information window provides a Server log.

The following sections provide information on each log file including a description of the log file, where the file is located, the log file archive behavior, and whether the log file is configurable.

- [Extreme Management Center Application Logs](#)
- [Syslog Log](#)
- [Traps Log](#)
- [Server Log](#)

## Extreme Management Center Application Logs

The Extreme Management Center application logs record alarm and event information for the Extreme Management Center Console application and any other Extreme Management Center applications you've enabled. You can view the application logs in the Extreme Management Center Event View. The Event View provides a separate tab for each application and displays the most recent 10,000 entries (table rows) for each log. Log files are automatically archived when their size reaches five megabytes and a new log file is opened. Archived log files are time-stamped and saved to the `<install directory>\NetSight\appdata\logs` directory.

You can use the Event Logs Options view (Tools > Options > Suite Options > Event Logs) to configure two application log file parameters. The "Number of Event Logs to Limit" option lets you set a limit to the number of application log files saved in the `logs` directory. The "Number of Rows to keep in table" option lets you set the number of entries (table rows) that will be displayed in the application logs (as well as the Traps log and the Syslog log) in the Event View.

## Syslog Log

The Syslog log shows events from devices that are configured to use the Extreme Management Center Syslog Server. The log records all the TFTP and BOOTP messages received for devices modeled in the Extreme Management Center database. You can view the Syslog log in the Extreme Management Center Event View. The Syslog log file is automatically archived at midnight each night or when the file reaches the maximum file size of one megabyte, and a new log file is opened. Archived log files are saved to the `<install directory>\NetSight\appdata\logs\syslogs` directory and a maximum of 10 files are saved.

On Windows systems, the Syslog file is configurable using the `.nssyslogd.cfg` file located in the `<install directory>\NetSight\services` directory. In the `.nssyslogd.cfg` file you can set the maximum file size and the maximum number of syslog files saved. On Linux systems, syslog is part of the operating system and is not configurable using an Extreme Management Center file.

In the Event Logs Options view (Tools > Options > Suite Options > Event Logs), the "Number of Rows to keep in table" option sets the number of entries (table rows) displayed in the Syslog log (as well as the application logs and the Traps log) in the Event View.

## Traps Log

The Extreme Management Center SNMPTrap Service (`snmptrapd`) receives SNMP trap and inform messages from your network devices and logs them into the Traps log. You can view the Traps log in the Extreme Management Center Event View.

You can use the `trapd.conf` file located in the `<install directory>\NetSight\services` directory to add new traps and configure event definitions.

In the Event Logs Options view (Tools > Options > Suite Options > Event Logs), the "Number of Rows to keep in table" option sets the number of entries (table rows) displayed in the Traps log (as well as the application logs and the Syslog log) in the Event View.

Traps log files have the following default archive parameters:

- A Traps log file is automatically archived when its size reaches one megabyte and a new log file is opened.
- A maximum of 10 Traps log files are saved to the `<install directory>\NetSight\appdata\logs\traps` directory.

These archive parameters can be changed by adding options to the beginning of the first line of the `nssnmptrapd.cfg` file located in the `<install directory>\NetSight\services` directory. Add the `-maxfiles` option to set the maximum number of files and/or add the `-maxsize` option to set the maximum size of the file (maximum size allowed is 2 gigabytes). The following example shows the first line of the file with the `-maxfiles` option set to a maximum number of 15 files and the `-maxsize` option set for a maximum file size of 100 megabytes.

```
-maxfiles 15 -maxsize 100000000 -O bs -n -p 162 -z "C:\Program
Files\Extreme Networks\NetSight\services" -o "C:\Program
Files\Extreme Networks\NetSight\appdata\logs\traps" -c
"C:\Program Files\Extreme
Networks\NetSight\appdata\snmptrapd.conf" -M "C:\Program
Files\Extreme Networks\NetSight\appdata\System\mibs;C:\Program
Files\Extreme Networks\NetSight\appdata\System\mibs\MyMibs" -m
SNMPv2-SMI;IF-MIB;all
```

## Server Log

The Server log displays all the events for the Extreme Management Center server. It can be viewed on the Server Log tab of the Server Information window (Tools > Server Information). A new Server log is created every day. Previous logs are dated and saved to the

`<install directory>\NetSight\appdata\logs` directory. If the Extreme Management Center Server is local, you can view previous logs using the File sub-tab on the Server Information tab in the Server Information window.

You can use the Event Logs Options view (Tools > Options > Suite Options > Event Logs) to limit the number of server log files saved in the `logs` directory. This can help you control total disk space usage.

You can configure Server log properties in the `log4j.xml` file located in the `<install directory>\NetSight\jboss\server\default\conf` directory.

# Device Manager Help

---

Device Manager provides comprehensive remote network management support for Extreme Networks products using Device Views to monitor your network devices. Device Views provide a graphic representation of the device, including a color-coded port display which informs you of the current status of all the ports on the device. Device Views also provide detailed device-level information, and serve as an access point to other device management windows. By clicking on various areas of the Device View, you can access menus with device- and port-level options, as well as utility applications for the device.



## Device View

---

The Device View provides a graphic representation of a device, including a color-coded port display which informs you of the current status of all the ports on the device. Device Views also provide device-level information, and serve as an access point to device management functions.

The X-Pedition Router XP-8000 (SSR-8) displayed below is an example of a typical Device View display. The Device View menu bar provides access to device-level management options, as well as utility applications such as Configuration Upload/Download. Click on ports in the Port Display area to access menus with port-level management options. In addition, the Device Information area provides important status and management information for the device. Device Views for other devices, and the menu options they offer, may vary slightly.

**NOTE:** N-Series device management support is available through the [Port View on Console's Properties tab](#). Although you can launch Device Manager on these devices, it is recommended that you use the Console Properties tab for device management of these devices.

Information on Device View features:

- [Menu Bar](#)
- [Port Display](#)
- [Device Information](#)

Sample Device View.

The screenshot shows a window titled "SSR-8 : 10.20.30.10" with a menu bar "Device View Utilities Help". The main area is divided into several sections:

- Port Grids:**
  - Port 7 (GSX):** A 2x2 grid with columns 1 and 2, and rows 1 and 2. All cells contain "NLK".
  - Port 4 (10TX):** A 1x8 grid with columns 1-8. All cells contain "NLK".
  - Port 2 (10TX):** A 1x8 grid with columns 1-8. Column 1 is "LNK" (green), column 2 is "LNK" (green), and columns 3-8 are "NLK" (yellow).
  - Port 3 (WAN):** A 1x4 grid with columns 1-4. All cells contain "NLK".
  - Port 1 (10FX):** A 1x8 grid with columns 1-8. All cells contain "NLK".
- System Information (Right Panel):**
  - Status: Up (indicated by a green arrow)
  - View: Link
  - Uptime: 0 Days 00:56:43
  - Base MAC: 00-E0-63-0B-B0-1A
  - Firmware: E8.2.0.A5
  - Boot Prom: E3.0.0.0
  - Device Date: 04/02/2001
  - Device Time: 08:47:44
- Port Selection Grid (Bottom Right):**

6	7
4	5
2	3
CM	CM/1
PS1	PS2

**NOTE:** The Link and Operational views will show a *DRMT* status for links that are attached to an active Link Aggregation Group (LAG).

**Related Information**

For information on related tasks:

- [How to Access a Device View](#)

## Menu Bar

---

The Device View menu bar provides access to device-level management options, as well as utility applications such as Configuration Upload/Download. The menu options may vary depending on the device being displayed.

Device View Utilities Help

### *Device Menu*

Click on **Device** in the Device View menu bar to display a menu with the following options. The menu options may vary depending on the device being displayed.

#### **Device > Device Information**

Displays a physical hardware description of the device.

#### **Device > VLAN > Bridge Extension Configuration**

Opens the [Bridge Extension Configuration window](#) where you can view the bridge extension functionality implemented on the device, and enable or disable Traffic Classes, GMRP, and GVRP at the device level (if supported).

#### **Device > VLAN > VLAN Configuration**

Opens the [VLAN Configuration](#) window where you can add and delete VLANs, configure VLAN IDs and names, and enable or disable VLANs.

#### **Device > VLAN > VLAN Port Configuration**

Opens the [VLAN Port Configuration \(Basic\) window](#) where you can configure basic VLAN port parameters such as VLAN name, egress state, and Acceptable Frame Types. You can also access advanced VLAN port parameters from this window.

#### **Device > VLAN > VLAN Egress Port Configuration**

Opens the [VLAN Egress Port Configuration window](#) which lets you select a VLAN on the device, and display the ports whose egress lists contain the selected VLAN. The window also allows you to change the egress state for each port.

#### **Device > VLAN > Bridge Extension Port Priority**

Opens the [Bridge Extension Port Priority window](#) where you can set the default Ingress User Priority for each port on a device.

**Device > VLAN > Bridge Extension Port Traffic Class**

Opens the [Bridge Extension Port Traffic Class window](#) where you can set the priority-to-traffic class mapping for each port on a device.

**Device > VLAN > Bridge Extension Port GARP Times**

Opens the [Bridge Extension Port GARP Times window](#) where you can configure GARP (Generic Attribute Registration Protocol) times for each port on a device.

**Device > VLAN > Bridge Extension Port GMRP**

Opens the [Bridge Extension Port GMRP window](#) where you can configure whether GMRP (GARP Multicast Registration Protocol) is enabled or disabled on each port.

**Device > MIB-II > Interface Summary**

Opens the [Interface Summary window](#) which provides an overview of interface information for each port on the device. You can also access detailed [Interface Statistics](#) from this window.

**Device > MIB-II > SNMP Group**

Opens the [SNMP Group window](#) where you can view statistical information concerning SNMP (Simple Network Management Protocol) defined objects on your device.

**Device > MIB-II > System Group**

Opens the [System Group window](#) where you can enter the device name, location, and contact person. You can also view the SysORTable which defines the Agents-Capabilities (A-C) statement for the device.

**Device > MIB-II > IP Group**

Opens the [IP Group window](#) where you can view a statistical breakdown of the number of datagrams received by and transmitted from the device.

**Device > MIB-II > IP Address Table**

Opens the [IP Address Table window](#) where you can verify port broadcast addresses, and reassembly guidelines for fragments. This window also displays IP addresses and subnet masks for ports on the device.

**Device > MIB-II > Net to Media**

Opens the [Net to Media window](#) where you can map IP addresses into physical addresses.

**Device > MIB-II > ICMP Group**

Opens the [ICMP Group window](#) where you can view the number and type of ICMP (Internet Control Message Protocol) messages received and

transmitted by the device.

#### Device > MIB-II > TCP Group

Opens the [TCP Group window](#) where you view the type of algorithm used to compute the retransmission of datagrams on your network. This window also displays the TCP (Transmission Control Protocol) connection state of the ports on your device.

#### Device > MIB-II > UDP Group

Opens the [UDP Group window](#) where you can view information concerning the transport protocol for your device. The window also displays a list of UDP (User Datagram Protocol) listeners, including their associated local IP address and port number.

#### Device > Bridge > Bridge Summary

Opens the [Bridge Summary window](#) where you can view the current status of bridging across your device and view information on each bridge port.

#### Device > Bridge > Bridge Filtering Database

Opens the [Bridge Filtering Database window](#) where you can add or delete entries from the Filtering Database and configure filtering information for each entry.

#### Device > Bridge > Bridge Spanning Tree

Opens the [Bridge Spanning Tree Configuration window](#) where you can view and modify bridge port- and device-level information relating to the Spanning Tree Algorithm.

#### Device > Bridge > Find Source Address

Opens the [Find Source Address window](#) used to locate the source port for a specific MAC address on the selected device.

#### Device > Ethernet Port Configuration

Opens the [Ethernet Port Configuration window](#) where you can view and configure the speed, duplex, flow control, and auto negotiation parameters for each port on the selected device.

#### Device > Broadcast Suppression

Opens the [Broadcast Suppression and Statistics window](#) where you can monitor the number of broadcast packets received by each interface, and configure the number of broadcast packets forwarded to other interfaces.

#### Device > Configure Com Port

Opens the [Com Port Configuration window](#) where you can configure a device's communications port(s).

**Device > Exit**

Closes the Device View.

*View Menu*

The Device View displays different port information depending on what View Menu option is selected. Click on **View** in the menu bar to display a menu with the following options.

**View > Link**

Displays the port's link state:

- **LNK** (green) -- Link
- **NLK** (yellow) -- No Link (the default port display when you open the Chassis View)
- **TST** (yellow) -- Testing mode
- **UNK** (yellow) -- Unknown, the device returns the value Unknown
- **UNK** (light gray) -- Unknown, the device is returning a value that the software does not recognize
- **DRMT** (yellow) -- Dormant; the interface is waiting for external actions (such as a serial line waiting for an incoming connection)  
**NOTE:** The Link view will show a *DRMT* status for links that are attached to an active Link Aggregation Group (LAG).
- **NPST** (yellow) -- Not Present; the interface has missing components (usually hardware)
- **DWN** (red) -- Lower Layer Down; the interface is down due to the state of lower-layer interface(s)
- **blank** (dark gray) -- the device is not responding

**View > Admin**

Displays the desired state of the interface:

- **ON** (green) -- the port has been administratively enabled
- **OFF** (red) -- the port has been administratively disabled
- **TST** (yellow)-- the port has been administratively placed in a test mode
- **UNK** (light gray) -- Unknown, the device is returning a value that the software does not recognize
- **blank** (dark gray) -- the device is not responding

### View > Operator

Displays the current operational state of the interface:

- **ON** (green) -- operational status up
- **OFF** (red) -- operational status down
- **TST** (yellow) -- operational status testing; no operational packets can be passed
- **UNK** (yellow) -- Unknown, the device returns the value Unknown
- **UNK** (light gray) -- Unknown, the device is returning a value that the software does not recognize
- **DRMT** (yellow) -- Dormant; the interface is waiting for external actions (such as a serial line waiting for an incoming connection)
  - **NOTE:** The Operational view will show a *DRMT* status for links that are attached to an active Link Aggregation Group (LAG).
- **NPST** (yellow) -- Not Present; the interface has missing components (usually hardware)
- **DWN** (red) -- Lower Layer Down; the interface is down due to the state of lower-layer interface(s)
- **blank** (dark gray) -- the device is not responding

### View > Load

Displays the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits/sec, or 1.00 Gbits/sec) of the connected network.

### View > Errors

Displays the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors generated during the last polling interval by devices connected to that port compared to the total number of packets processed by the port.

### View > I/F Mapping

Displays the interface index associated with each port.

### View > I/F Speed

Displays the bandwidth of each individual port: i.e., 10M (megabits) for standard Ethernet, 100M for Fast Ethernet, and 1.00G for Gigabit Ethernet.

**View > I/F Type**

Displays the interface type, for example, Ethernet (ETH). There is no type distinction between Ethernet, Fast Ethernet, or Gigabit Ethernet.

**View > Refresh**

Updates the information displayed in the Device View.

*Utilities Menu*

Click on **Utilities** in the Device View menu bar to display a menu with the following options. The menu options may vary depending on the device being displayed.

**Utilities > Configuration Upload/Download**

Opens the [Configuration Upload/Download window](#) where you can upload or download a configuration file.

**Utilities > Firmware Image Download**

Opens the [Firmware Image Download window](#) where you can download a new firmware image.

**Utilities > Options**

Opens the Device Manager Options window where you can specify polling options and the colors you want to use in Device Manager tables.

*Help Menu*

Click on **Help** in the Device View menu bar to display a menu with the following options.

**Help > MIB Information**

Displays the [MIB Information window](#) that provides useful information for troubleshooting Device Manager functionality.

**Help > Help Topics**

Displays the NetSight Help topics.

**Help > Release Notes**

Displays the NetSight Release Notes for the current release.

**Help > About This Window**

Displays detailed information about the Device View window.

**Help > About Device Manager**

Displays the NetSight Device Manager version and copyright information.



## Related Information

For information on related windows:

- [Device View](#)

# Port Display

The Port Display area of a Device View displays the modules and ports of the device being displayed. Click on ports in the Port Display area to access menus with port-level management options.

*Sample Port Display.*

7	GSX	1	2																				
		N	N																				
		L	L																				
		K	K																				
4	100TX	1	2	3	4	5	6	7	8														
		N	N	N	N	N	N	N	N														
		L	L	L	L	L	L	L	L														
		K	K	K	K	K	K	K	K														
2	100TX	1	2	3	4	5	6	7	8	3	WAN	1	2	3	4								
		L	L	N	N	N	N	N	N			N	N	N	N								
		N	N	L	L	L	L	L	L			L	L	L	L								
		K	K	K	K	K	K	K	K			K	K	K	K								
0	CM2									1	100FX	1	2	3	4	5	6	7	8				
												N	N	N	N	N	N	N	N				
												L	L	L	L	L	L	L	L				
												K	K	K	K	K	K	K	K				

**Module/Device Number**  
Click on the module/device number to access the [Module/Device Menu](#).

**Module/Device Type**  
Displays an abbreviated physical hardware description of the module or device.

**Port Number**  
Displays the port number on the module. Click on the port number to access the [Port Menu](#).

**Port Display**  
Ports display different information depending on what [View Menu](#) port display option is selected. The display is color-coded for three of the options: [Link](#), [Admin](#), and [Operator](#). All other options will continue to reflect the most recently selected option that does use color-coding. Click on a port to access the [Port Menu](#).

### *Module/Device Menu*

Click on a module/device number in the Port Display to display a menu with the following option.

#### **Board Type**

Displays a physical hardware description of the module/device and the firmware version.

### *Port Menu*

Click on a port in the Port Display to display a menu with the following options. The menu options may vary depending on the device being displayed.

#### **Interface Statistics**

Displays the [Interface Statistics window](#) where you can view color-coded statistical information about the port.

#### **RMON Ethernet Statistics**

Displays the [RMON Ethernet Statistics window](#) where you can view a detailed statistical breakdown of traffic on the monitored Ethernet network segment. RMON must be enabled through the device's local management.

#### **RMON History List**

Displays the [RMON History List window](#) where you can view a list of RMON history tables for a selected port (interface). RMON must be enabled through the device's local management.

#### **Port Type**

Displays a description of the port.

#### **IF Enable/Disable**

Administratively turns the port (interface) on or off.

---

### **Related Information**

For information on related windows:

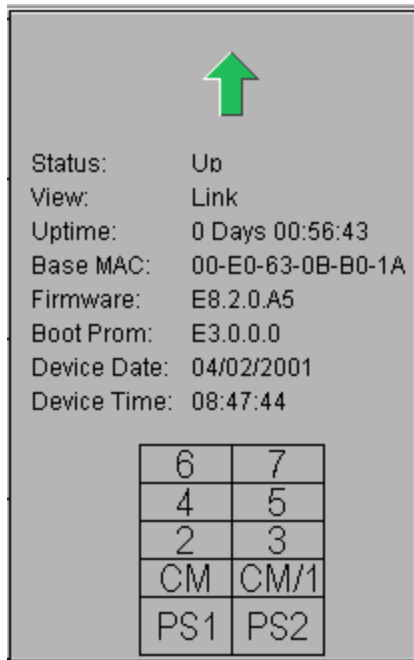
- [Device View](#)

## Device Information

---

The Device Information area of a Device View provides important management information such as device status, MAC address, and firmware version.

### Sample Device Information.



### Status

Displays the connection status: Up, Down, Standby, or Unknown.

### View

Indicates the [View Menu](#) port display option currently in effect.

### Uptime

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

### Base MAC

The physical layer address assigned to the interface through which Device Manager is communicating. MAC addresses are hard-coded in the device, and are not configurable.

### Firmware

The revision of device firmware stored in the device's flash PROMs.

**Boot Prom**

The revision of Boot Prom installed in the device.

**Hardware**

Displays the hardware version.

**Device Date**

Displays the current date in the internal clock of the device.

**Device Time**

Displays the current time in hh:mm:ss format, in the internal clock of the device.

**Device Display**

A graphical depiction of the device layout indicating the slot numbers, control modules, and power supplies. Not all Device Views will show this display.

---

**Related Information**

For information on related windows:

- [Device View](#)

## How To Use Device Manager

---

The **How To** help section contains help topics that give you instructions for performing tasks in Device Manager.

## How to Access a Device View

---

A Device View provides a graphic representation of a monitored device, detailed device management information, and also serves as an access point to other device management windows.

1. Select a device in Console's left panel tree, and right-clicking the device and selecting Device Manager from the menu. The Device View opens.
- 

### Related Information

For information on related windows:

- [Device View](#)

## How to Add or Modify a VLAN

---

Use the [VLAN Configuration window](#) to modify an existing VLAN or to add a new VLAN to the device.

Instructions on:

- [Adding a VLAN](#)
- [Modifying a VLAN](#)

### *Adding a VLAN*

You can add a new VLAN to the device using the VLAN Configuration window.

1. Select **Device > VLAN > VLAN Configuration** from the Device View menu bar. The [VLAN Configuration window](#) opens.
2. In the VLAN ID field, enter the number you want to use to identify the VLAN. Allowable values range from 2 to 4094. VLAN ID 1 is reserved for the default VLAN and cannot be used.
3. In the VLAN Name field, enter the name (up to 32 characters) that you want to assign to the VLAN.
4. Select the desired administrative status for the VLAN: Enabled or Disabled.
5. Click **Apply** to add the new VLAN.

### *Modifying a VLAN*

You can modify a VLAN's name and administrative status using the VLAN Configuration window.

1. Select **Device > VLAN > VLAN Configuration** from the Device View menu bar. The [VLAN Configuration window](#) opens.
  2. Select the desired VLAN from the Configured VLANs list.
  3. In the VLAN Name field, enter the new name (up to 32 characters) that you want to assign to the VLAN.
  4. Select the desired administrative status for the VLAN: Enabled or Disabled.
  5. Click on **Apply** to set the changes.
- 

## Related Information

For information on related tasks:



- [How to Configure Port Egress State](#)

For information on related windows:

- [VLAN Configuration Window](#)
- [VLAN Egress Port Configuration Window](#)
- [VLAN Port Configuration \(Advanced\) Window](#)
- [VLAN Port Configuration \(Basic\) Window](#)

## How to Configure a Bridge Filtering Database

---

The Filtering Database (which makes up the IEEE 802.1 Source Address Table) is used to determine how frames are forwarded or filtered across the device's bridge ports. You can add or delete entries (source addresses) from the device's Filtering Database and configure filtering information for each entry using the [Bridge Filtering Database window](#). Filtering information specifies the set of ports to which frames received from a specific port, and containing a specific destination address, are allowed to be forwarded.

The Filtering Database is made up of two separate databases: Static and Learned. The Static database contains source addresses that are entered by a network administrator. The Learned database consists of source addresses that accumulate as part of the learning process. The device learns network addresses by entering the source address and port association of each received frame into the Filtering Database.

The device uses the Filtering Database to determine how to forward frames. It examines each received frame, and checks to see if the frame's destination address matches a source address listed in the Filtering Database. If there is a match, the device uses the filtering information for that source address to determine how to forward or filter the frame.

Instructions on:

- [Configuring Filter Information](#)
- [Deleting an Address](#)
- [Setting the Age Time](#)

### *Configuring Filter Information*

You can configure filtering information for each source address entry in the Filtering Database. When you configure the filtering information, you must specify a Source Address, Status Type and Receive port, and specify the set of Destination ports to which frames received from the specified Receive port and destined for the selected Source Address, are allowed to be forwarded or filtered.

1. Select **Device > Bridge > Bridge Filtering Database** from the Device View menu bar. The [Bridge Filtering Database window](#) opens. The left side of the window displays the Source Address Information which is a table of

addresses in the Filtering Database. The right side of the window displays the Configure Address Filter area where you enter filtering information. For detailed information on the table and its fields, see the Bridge Filtering Database window.

2. **In the Source Address field**, enter the source MAC address. You can enter a new source address, or configure an existing address by clicking on the desired address in the Source Address Information table.
3. **In the Status Type field**, use the drop-down list to select the desired status type. In order to configure filtering information, you must select a status type of Permanent, Dynamic, or Static. You cannot configure filtering for Learned or Self addresses.
  - **Permanent** -- Permanent addresses are manually added to the Static Database via the Filtering Database window, and remain in the database even when the device is shutdown or restarted.
  - **Static** -- Static addresses are manually added to the Static Database via the Filtering Database window, and remain in the database until the device is restarted.
  - **Dynamic** -- Dynamic addresses are manually added to the Static Database via the Filtering Database window. Use the Age Time feature to set the time period that these addresses remain in the database.
4. **In the Receive Port field**, use the drop-down list to select the desired Receive Port. The Receive port is the port on which a frame must be received in order for the source address filter information to apply. You can specify one Receive port for each source address entry, or you can specify "All Ports" as Receive ports. Since a Receive port must be specified when you change a status type, Device Manager automatically selects All Ports as the Receive Port value unless you specify another value. (If All Ports is selected, an asterisk (\*) will be displayed in the Receive Port column of the Source Address Information table.)
5. **In the Destination Ports Table**, configure the port(s) to which frames received from the specified Receive port and destined for the selected Source Address, are allowed to be forwarded. The Destination Ports table indicates the forwarding or filtering (blocking) action for each destination port. The Current Column displays the currently configured action and the Static column displays the desired action. Select the destination port, then right-click and select the desired action from the menu:

- **Forward** -- forward traffic out the Destination port to the Source Address entry.
  - **Block** -- block traffic out the Destination port to the Source Address entry.
  - **Forward on All Ports** -- forward traffic out all Destination ports to the Source Address entry.
  - **Block on All Ports** -- block traffic out all Destination ports to the Source Address entry. This is the default value when no forwarding/filtering information is configured when changing the status type and Receive port for a Source Address entry.
6. Click **Apply** to apply the filtering configuration information.

### *Deleting an Address*

You can delete a Permanent, Dynamic, or Static source address entry from the Filtering Database. Self and Learned address entries cannot be deleted.

1. Select **Device > Bridge > Bridge Filtering Database** from the Device View menu bar. The [Bridge Filtering Database window](#) opens.
2. Select the desired address from the table.
3. Click **Delete** to delete the address from the database.

### *Setting the Age Time*

The Age Time is the length of time, in seconds, that Dynamic and Learned addresses in the Source Address Table remain active before they are dropped from the database. Allowable values range from 10 to 1000000 seconds.

1. Select **Device > Bridge > Bridge Filtering Database** from the Device View menu bar. The [Bridge Filtering Database window](#) opens.
2. In the Age Time field, enter the new Age Time, in seconds. Allowable values range from 10 to 1000000 seconds.
3. Click **Apply** to set the new Age Time.

---

## **Related Information**

For information on related windows:

- [Bridge Filtering Database Window](#)

## How to Configure Port Egress State

---

Use the [VLAN Egress Port Configuration window](#) to configure port egress state. The port egress state determines how frames are forwarded out the port.

1. Select **Device > VLAN > VLAN Egress Port Configuration** from the Device View menu bar. The VLAN Egress Port Configuration window opens.
2. Select the desired VLAN from the Selected VLAN list at the top of the window.
3. In the Port Egress Information list, right-click the desired port to select how the frames are transmitted: No Egress (frames are not transmitted), Tagged (frames are transmitted as tagged), Untagged (frames are transmitted as untagged).
4. To change the egress state for all the ports listed, right-click a port and select All No Egress, All Tagged, or All Untagged.
5. Click **Apply** to set the port egress state.

**NOTE:** On the X-Pedition Router, Access ports cannot be set to tagged, and Trunk ports cannot be set to untagged. Egress state cannot be set by the user on X-Pedition Routers with firmware versions of E8.1.0.0 or earlier.

---

### Related Information

For information on related tasks:

- [How to Add or Modify a VLAN](#)

For information on related windows:

- [VLAN Configuration Window](#)
- [VLAN Egress Port Configuration Window](#)
- [VLAN Port Configuration \(Advanced\) Window](#)
- [VLAN Port Configuration \(Basic\) Window](#)

## How to Find a Source Address

---

Use the [Find Source Address window](#) to locate the source port for a specific MAC address on a device. When you perform a Find operation, the device's Filtering Database is searched for the specified MAC address. If it is found, the Component field will display the value "Bridge" indicating that the address was found on a bridging interface. The Port Instance field will display the index number assigned to the bridge port on which the address was located.

---

**NOTE:** Bridge port index numbers may not match interface port index numbers (the MIB-II *ifIndex* value) because there is an offset in the mapping between the two. Use MIB Tools to query *dot1dBasePortIfIndex*(1.3.6.1.2.1.17.1.4.1.2) and view the mapping and offset.

---

1. Select **Device > Bridge > Find Source Address** from the Device View menu bar. The Find Source Address Window opens.
  2. In the **Enter Address** field, enter the address you want to find, in XX-XX-XX-XX-XX-XX format. If you enter **All**, the Port Instance for every entry in the device's Filtering Database will be displayed.
  3. Click **Find** to locate the selected address. The device component and the port instance where the selected address is located appears in the window.
- 

### Related Information

For information on related windows:

- [Find Source Address Window](#)

## Device Manager Windows

---

The **Windows** help section contains help topics describing Device Manager windows and their field definitions.

## Bridge Extension Configuration Window

Use this window to view the bridge extension functionality implemented on the device, and to enable or disable Traffic Classes, GMRP, and GVRP at the device level (if supported).

The Bridge MIB (Management Information Base) Extensions provide functionality for managing the traffic class and multicast filtering components of IEEE 802.1D, and for managing IEEE 802.1Q VLANs. Not every device supports the Bridge MIB Extensions. Access **Help > Device Information** for MIB and feature support information.

To access the Bridge Extension Configuration window, select **Device > VLAN > Bridge Extension Configuration** from the Device View menu bar.

**Bridge Extension Configuration: 10.20.30.40**

**Bridge Capability**

Extended Multicast Filtering Services	Yes
Traffic Classes	Yes
Static Entry Individual Port	No
VLAN Learning	IVL/SVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

**Bridge Port Capability**

Port	VLAN Tagging	Configure Frame Types ^	Ingress Filtering
23	No	No	No
24	No	No	No
25	No	No	No
26	No	No	No
27	No	No	No
28	No	No	No
1	Yes	Yes	Yes
2	Yes	Yes	Yes
3	Yes	Yes	Yes
4	Yes	Yes	Yes
5	Yes	Yes	Yes
6	Yes	Yes	Yes
7	Yes	Yes	Yes
8	Yes	Yes	Yes
9	Yes	Yes	Yes
10	Yes	Yes	Yes
11	Yes	Yes	Yes

Buttons: Close, Refresh, Help

Edit Mode.

### *Bridge Capability Area*

These fields indicate whether the device implements certain IEEE 802.1D and 802.1Q functionality.

### Extended Multicast Filtering Services

Devices that implement this functionality can perform filtering of individual multicast addresses controlled by GMRP (GARP Multicast Registration



Protocol). GMRP is a protocol used to register multicast addresses on ports to control flooding of multicast frames.

### **Traffic Classes**

Devices that implement this functionality can map user priority to multiple traffic classes. Priority is mapped to a specific traffic class (queue number), and frames are transmitted based on what queue they are in. Frames in the highest numbered queue are transmitted out a port first. The number of traffic queues supported varies depending on the switch.

### **Static Entry Individual Port**

Allows you to specify ports that frames must be received from for filtering information to apply.

### **VLAN Learning**

Displays the filtering database modes of operation implemented by the device:

- **IVL** -- Independent VLAN Learning
- **SVL** -- Shared VLAN Learning
- **IVL/SVL** -- Both Independent and Shared VLAN Learning

### **Configurable PVID Tagging**

Devices that implement this functionality have the ability to override the default PVID setting and the egress state (Tagged or Untagged) on each port.

### **Local VLAN Capable**

Devices that implement this functionality can support multiple local bridges, outside of the scope of 802.1Q defined VLANs.

### **Traffic Classes**

These fields display whether Traffic Classes (queues) are currently enabled or disabled on the device and allow you to change the setting. When Traffic Classes are enabled, the device can map user priority to specific traffic queues.

### **GMRP**

These fields display whether GMRP (GARP Multicast Registration Protocol) is currently enabled or disabled on the device and allow you to change the setting. GMRP is a protocol used to register multicast addresses on ports to control flooding of multicast frames.

## GVRP

These fields display whether GVRP (GARP VLAN Registration Protocol) is currently enabled or disabled on the device and allow you to change the setting. GVRP is a protocol used to dynamically add VLANs to port egress lists across a domain.

## *Bridge Port Capability Area*

This table lists the ports on the device and whether they implement certain IEEE 802.1D and 802.1Q functionality. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### Port

Displays the number that identifies the port.

### VLAN Tagging

Ports that implement this functionality support 802.1Q VLAN tagging of frames and GVRP (GARP VLAN Registration Protocol).

### Configure Frame Types

Ports that implement this functionality allow you to configure the port's Acceptable Frame Type. This setting specifies whether a port will accept both tagged and untagged frames, or only tagged frames.

### Ingress Filtering

Ports that implement this functionality support the discarding of any frame received on a port whose VLAN classification is not on that port's egress list.

---

## Related Information

For information on related windows:

- [Bridge Extension Port Priority](#)
- [Bridge Extension Port Traffic Class](#)
- [Bridge Extension Port GARP Times](#)
- [Bridge Extension Port GMRP](#)

## Bridge Extension Port GARP Times Window

Use this window to configure Generic Attribute Registration Protocol (GARP) times for each port. GARP is a protocol that is used to propagate port state and/or user information throughout a switched network. GARP time values are used by all GARP applications running on the device (e.g. GVRP and GMRP).

To access the Bridge Extension Port GARP Times window, select **Device > VLAN > Bridge Extension Port GARP Times** from the Device View menu bar.

Bridge Extension Port GARP Times: 10.20.30.40

Configured Port GARP Times:

IP Address	Port	Join Time	Leave Time	Leave All Time
10.20.30.40	1	20	60	1000
10.20.30.40	2	20	60	1000
10.20.30.40	3	20	60	1000
10.20.30.40	4	20	60	1000
10.20.30.40	5	20	60	1000
10.20.30.40	6	20	60	1000
10.20.30.40	7	20	60	1000
10.20.30.40	8	20	60	1000
10.20.30.40	9	20	60	1000
10.20.30.40	10	20	60	1000
10.20.30.40	11	20	60	1000
10.20.30.40	12	20	60	1000

Join Time (centiseconds):

Leave Time (centiseconds):

Leave All Time (centiseconds):

Edit Mode.

### *Configured Port GARP Times*

This table displays the Generic Attribute Registration Protocol (GARP) times configured for each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**IP Address**

Displays the IP address.

**Port**

Displays the number that identifies the port.

**Join Time**

Displays the Join Time configured for the port. Join Time is the maximum time period of GARP PDU (Protocol Data Unit) transmits (to register an attribute).

**Leave Time**

Displays the Leave Time configured for the port. Leave Time is the period of time from which an attribute is registered as not required (leaving), to not present (empty).

**Leave All Time**

Displays the Leave All Time configured for the port. This is the period of time at which Leave All PDUs are generated, which force the recipients to respond by registering for their active attributes.

**Join Time (centiseconds)**

Use this field to enter the amount of join time in centiseconds.

**Leave Time (centiseconds)**

Use this field to enter the amount of leave time in centiseconds.

**Leave All Time (centiseconds)**

Use this field to enter the amount of leave all time in centiseconds.

---

**Related Information**

For information on related windows:

- [Bridge Extension Configuration](#)
- [Bridge Extension Port Priority](#)
- [Bridge Extension Port Traffic Class](#)
- [Bridge Extension Port GMRP](#)

## Bridge Extension Port GMRP Window

Use this window to configure whether GMRP (GARP Multicast Registration Protocol) is enabled or disabled on each port. GMRP is a protocol used to register multicast addresses on ports to control flooding of multicast frames.

To access the Bridge Extension Port GMRP window, select **Device > VLAN > Bridge Extension Port GMRP** from the Device View menu bar.

Bridge Extension Port GMRP: 10.20.30.40

Port GMRP information:

IP Address	Port	Status	Failed Registration	Last PDU Origin
10.20.30.40	1	Enabled	0	00-00-00-00-00-00
10.20.30.40	2	Enabled	0	00-00-00-00-00-00
10.20.30.40	3	Enabled	0	00-00-00-00-00-00
10.20.30.40	4	Enabled	0	00-00-00-00-00-00
10.20.30.40	5	Enabled	0	00-00-00-00-00-00
10.20.30.40	6	Enabled	0	00-00-00-00-00-00
10.20.30.40	7	Enabled	0	00-00-00-00-00-00
10.20.30.40	8	Enabled	0	00-00-00-00-00-00
10.20.30.40	9	Enabled	0	00-00-00-00-00-00
10.20.30.40	10	Enabled	0	00-00-00-00-00-00
10.20.30.40	11	Enabled	0	00-00-00-00-00-00
10.20.30.40	12	Enabled	0	00-00-00-00-00-00
10.20.30.40	13	Enabled	0	00-00-00-00-00-00

GMRP Status:

Edit Mode.

### *Port GMRP Information*

This table displays whether GMRP (GARP Multicast Registration Protocol) is enabled or disabled on each port. It also displays the total number of failed GMRP registrations for all VLANs on each port, and the source MAC Address of the last GMRP message (PDU, Protocol Data Unit) received on each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**IP Address**

Displays the IP address.

**Port**

Displays the number that identifies the port.

**Status**

Displays whether GMRP (GARP Multicast Registration Protocol) is disabled or enabled on the port.

**Failed Registration**

Displays the total number of failed GMRP registrations for all VLANs on the port.

**Last PDU Origin**

Displays the source MAC Address of the last GMRP message (PDU, Protocol Data Unit) received on the port.

**GMRP Status**

Use the drop-down list to enable or disable GMRP on the selected port.

---

**Related Information**

For information on related windows:

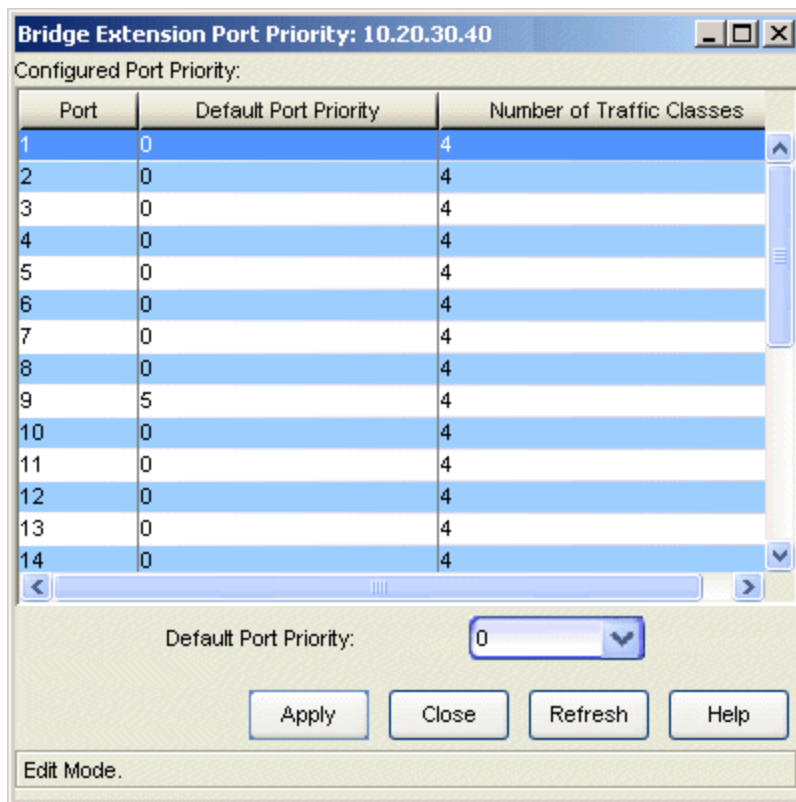
- [Bridge Extension Configuration](#)
- [Bridge Extension Port Priority](#)
- [Bridge Extension Port Traffic Class](#)
- [Bridge Extension Port GARP Times](#)

## Bridge Extension Port Priority Window

Use this window to set the default Ingress User Priority for each port. Priority is a value between 0 and 7 assigned to each frame, with 7 being the highest priority. Priority is used to assign frames transmission priority over other frames. Frames assigned higher priority are transmitted before frames with a lower priority. If a frame received on a port does not have a priority assigned to it (and no priority classification rule exists), it is assigned the default Ingress User Priority.

The window also displays the number of traffic classes (queues) supported for each port.

To access the Bridge Extension Port Priority window, select **Device > VLAN > Bridge Extension Port Priority** from the Device View menu bar.



Port	Default Port Priority	Number of Traffic Classes
1	0	4
2	0	4
3	0	4
4	0	4
5	0	4
6	0	4
7	0	4
8	0	4
9	5	4
10	0	4
11	0	4
12	0	4
13	0	4
14	0	4

Default Port Priority: 0

Apply Close Refresh Help

Edit Mode.

### *Configured Port Priority*

This table displays the default Ingress User Priority configured for each port. If a frame received on a port does not have a priority assigned to it (and no priority classification rule exists), it is assigned the default Ingress User Priority. The table

also displays the number of traffic classes (queues) supported for each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**Port**

Displays the number that identifies the port.

**Default Ingress User Priority**

Displays the default Ingress User Priority assigned to the port. Priority is a value between 0 and 7 assigned to each frame, with 7 being the highest priority.

**Number of Traffic Classes**

Displays the number of egress Traffic Classes (queues) supported by the port. The number of traffic queues supported varies depending on the switch.

**Port**

Use the drop-down list to select the desired port.

**Default Ingress User Priority**

Use the drop-down list to select the desired priority: 0-7, with 7 being the highest priority.

---

**Related Information**

For information on related windows:

- [Bridge Extension Configuration](#)
- [Bridge Extension Port Traffic Class](#)
- [Bridge Extension Port GARP Times](#)
- [Bridge Extension Port GMRP](#)



## Bridge Extension Port Traffic Class Window

---

Use this window to set the priority-to-traffic class mapping for each port. The window displays the number of traffic classes supported by each port and allows you to map a priority to a specific traffic class.

Switches transmit frames based on the frame's transmission priority. Priority is a value between 0 and 7 assigned to each frame with 7 being the highest priority. Frames assigned a higher priority are transmitted before frames with a lower priority. A switch maps each priority number to a specific traffic class (queue number), and transmits frames based on what queue they are in. Frames in the highest numbered queue are transmitted out a port first. The number of traffic queues supported varies depending on the switch, either four (0-3) or two (0-1) traffic queues.

To access the Bridge Extension Port Traffic Class window, select **Device > VLAN > Bridge Extension Port Traffic Class** from the Device View menu bar.

Bridge Extension Port Traffic Class: 10.20.30.40

Configured Port Traffic Class:

Port	Priority	Number of Traffic Classes (queues)	Traffic Class (queue number)
1	0	4	1
1	1	4	0
1	2	4	0
1	3	4	1
1	4	4	2
1	5	4	2
1	6	4	3
1	7	4	3
2	0	4	1
2	1	4	0
2	2	4	0
2	3	4	1
2	4	4	2
2	5	4	2
2	6	4	3
2	7	4	3
3	0	4	1
3	1	4	0
3	2	4	0
3	3	4	1
3	4	4	2

Map to Traffic Class: 1

Apply Close Refresh Help

Edit Mode.

### Configured Port Traffic Class

This table displays the priority-to-traffic class mapping for each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

#### Port

Displays the number that identifies the port.

#### Priority

Priority is a value between 0 and 7 with 7 being the highest priority. Switches transmit frames based on the frame's transmission priority. Frames assigned a higher priority are transmitted before frames with a lower priority. Priority is mapped to a specific class (queue number), and

frames are transmitted based on what queue they are in. Frames in the highest numbered queue are transmitted out a port first. The number of traffic queues supported varies depending on the switch, either four (0-3) or two (0-1) traffic queues.

**Number of Traffic Classes (queues)**

Displays the number of Traffic Classes (queues) supported by that port. The number of traffic queues supported varies depending on the switch, either four (0-3) or two (0-1) traffic queues.

**Traffic Class (queue number)**

Displays the Traffic Class mapped to the port priority. Priority is mapped to a specific Traffic Class (queue number), and frames are transmitted based on what queue they are in. Frames in the highest numbered queue are transmitted out a port first.

**Map to Traffic Class**

Use this drop-down list to select the desired traffic class (queue number) for the selected port priority.

---

**Related Information**

For information on related windows:

- [Bridge Extension Configuration](#)
- [Bridge Extension Port Priority](#)
- [Bridge Extension Port GARP Times](#)
- [Bridge Extension Port GMRP](#)

## Bridge Filtering Database Window

---

The Filtering Database (which makes up the IEEE 802.1 Source Address Table) is used to determine how frames are forwarded or filtered across the device's bridge ports. You can use this window to add or delete entries (source addresses) from the Filtering Database and configure filtering information for each entry. Filtering information specifies the set of ports to which frames received from a specific port, and containing a specific destination address, are forwarded.

The Filtering Database is made up of two separate databases: Static and Learned. The Static database contains source addresses that are entered by a network administrator. The Learned database consists of source addresses that accumulate as part of the learning process. The device learns network addresses by entering the source address and port association of each received frame into the Filtering Database. The Learned Database holds a maximum of 4000 addresses.

The device uses the Filtering Database to determine how to forward frames. It examines each received frame, and checks to see if the frame's destination address matches a source address listed in the Filtering Database. If there is a match, the device uses the filtering/forwarding information for that source address to determine how to forward or filter the frame.

To access the Bridge Filtering Database window, select **Device > Bridge > Bridge Filtering Database** from the Device View menu bar.

**Bridge Filtering Database: 10.20.30.40**

Source Address Information

List Type	Number	Age Time [seconds]
Permanent:	2	Permanent
Static:	0	On Reset
Dynamic:	0	300 <input type="button" value="Apply"/>
Learned [Read Only]:	54	

Source Address	Status Type	Source Port	Receive Port	Destination Ports
00-00-1D-C3-85-69	Permanent	?	4	00-00-00-00
00-00-1D-C3-85-69	Permanent	?	7	60-00-00-00
00-00-1D-1D-B1-0E	Learned	11	N/A	N/A
00-00-1D-24-87-19	Learned	21	N/A	N/A
00-00-1D-3C-5A-04	Learned	11	N/A	N/A
00-00-1D-3C-5A-1C	Learned	11	N/A	N/A
00-00-1D-46-39-E9	Learned	19	N/A	N/A
00-00-1D-54-EE-4C	Learned	19	N/A	N/A
00-00-1D-5B-CD-22	Learned	19	N/A	N/A
00-00-1D-65-18-5B	Learned	11	N/A	N/A
00-00-1D-83-77-33	Self	?	N/A	N/A
00-00-1D-86-9B-74	Learned	15	N/A	N/A
00-00-1D-87-8F-58	Learned	19	N/A	N/A

Configure Address Filter

Source Address: 00-00-1D-C3-85-69

Status Type: Permanent

Source Port: 5

Receive Port: 4

Destination Ports:

Port	Current	Static
1	Block	Block
2	Block	Block
3	Block	Block
4	Block	Block
5	Block	Block
6	Block	Block
7	Block	Block
8	Block	Block
9	Block	Block
10	Block	Block
11	Block	Block
12	Block	Block
13	Block	Block

Edit Mode.

### Source Address Information Area

This area displays the entries in the Filtering Database and lets you set the Age Time for Dynamic and Learned entries. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### List Type

Lists the total number and age time for the four database entry types: Permanent, Static, Dynamic, or Learned.

### Permanent

Displays the total number of permanent addresses in the Filtering Database. Permanent addresses are manually added to the Static Database using this window, and are stored in the battery-backed RAM of the device. Since they remain in the database on device shutdown or restart, their Age Time is "Permanent".

**Static**

Displays the total number of static addresses in the Filtering Database. Static addresses are manually added to the Static Database using this window. Since they remain in the database until the device is restarted, their Age Time is "On Reset".

**Dynamic**

Displays the total number of dynamic addresses in the Filtering Database. Dynamic addresses are manually added to the Static Database using this window. Use the [Age Time](#) feature to set the time period that these addresses remain in the Source Address Table.

**Learned (Read Only)**

Displays the total number of learned addresses in the Filtering Database. Learned addresses are added to the Learned Database through the learning process. The device learns network addresses by entering the source address and port association of each received frame into the Filtering Database. Use the [Age Time](#) feature to set the time period that these addresses remain in the Source Address Table. Learned address entries are divided into two types: Learned and Self.

- **Learned** -- These address entries have transmitted frames destined for a device attached to a device port's connected segment.
- **Self** -- These address entries have transmitted frames with a destination address of one of the device's bridging ports.

You cannot configure filtering/forwarding information for Learned or Self addresses.

**Number**

Displays the number of Permanent, Static, Dynamic, and Learned address entries currently in the database.

**Age Time (seconds)**

Displays the length of time, in seconds, that Dynamic and Learned addresses remain in the database before they are dropped. Allowable values range from 10 to 1000000 seconds. To change the Age Time, enter a new time in the field and click **Apply**. Permanent addresses are never dropped from the database, and Static addresses are dropped when the device is reset.

**Source Address**

Displays the MAC addresses for which the Bridge Filtering Database has filtering/forwarding information. The device checks each received frame to see if the frame's destination address matches a source address listed in

the Filtering Database. If there is a match, the device uses the filtering/forwarding information for that source address to determine how to filter or forward the frame.

### Status Type

Displays the type of database entry:

- **Permanent** -- Permanent addresses are manually added to the Static Database using this window, and remain in the database even when the device is shutdown or restarted.
- **Static** -- Static addresses are manually added to the Static Database using this window, and remain in the database until the device is restarted.
- **Dynamic** -- Dynamic addresses are manually added to the Static Database using this window. Use the Age Time feature to set the time period that these addresses remain in the database.
- **Learned** -- Learned addresses are added to the Learned Database through the learning process. The device learns network addresses by entering the source address and port association of each received frame into the Filtering Database. Learned address entries have transmitted frames destined for a device attached to a device port's connected segment. Use the Age Time feature to set the time period that these addresses remain in the database.
- **Self** -- Self addresses are added to the Learned Database through the learning process. The device learns network addresses by entering the source address and port association of each received frame into the Filtering Database. Self address entries have transmitted frames with a destination address of one of the device's bridging ports. Use the Age Time feature to set the time period that these addresses remain in the database.

### Source Port

Learned and Self entries display the port number on which the address entry was first detected. A question mark (?) indicates that the entry is a created Permanent, Dynamic, or Static entry, and has corresponding filtering information.

### Receive Port

Displays the number of the port on which a frame must be received in order for the source address filter/forward information to apply. You can specify one or multiple receive ports for each source address, or you can specify

"all ports" as receive ports. An asterisk (\*) indicates that the port filtering information applies to all ports (assuming there are no conflicting entries).

### Destination Ports

The set of ports to which frames received from the specified Receive port and destined for the selected Source Address, are allowed to be forwarded. The value is a hexadecimal notation with each octet specifying a set of eight ports: the first octet specifies ports 1 through 8, the second octet specifies ports 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port. Thus, each bridge port is represented by a single bit. If that bit has a value of '1' then that port is included in the set of ports; the port is not included if its bit has a value of '0'. (The setting of the bit corresponding to the Receive port is irrelevant.)

### Delete

Select an entry in the table and click **Delete** to remove the address from the database. Learned and Self address entries cannot be deleted.

### *Configure Address Filter Area*

This area allows you to configure the filtering/forwarding information for a source address. Select the desired address in the Source Address Information table (in this window). In order to configure filtering/forwarding information, an entry must have a status type of Permanent, Dynamic, or Static.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### Source Address

Displays the address selected in the Source Address Information Table (in this window) and allows you to configure filtering/forwarding information for that address.

### Status Type

Use the drop-down list to select the desired status type. In order to configure filtering/forwarding information, you must select a status type of Permanent, Dynamic, or Static. You cannot configure filtering/forwarding for Learned or Self addresses.



---

**NOTE:** Since a [Receive port](#) must be specified when you change a status type, Device Manager automatically selects All Ports as the Receive Port value unless you specify another value.

---

### Source Port

Learned and Self entries display the port number on which the address entry was first detected. A question mark (?) indicates that the entry is a created Permanent, Dynamic, or Static entry, and has corresponding filtering/forwarding information.

### Receive Port

Use the drop-down list to select the desired Receive port. A frame must be received on the specified Receive port for the filtering/forwarding action to apply. You can specify multiple Receive ports for each source address by creating separate entries for each port, or you can specify "All Ports" as receive ports.

---

**NOTE:** Since a Receive port must be specified when you change a status type, Device Manager automatically selects All Ports as the Receive Port value unless you specify another value.

---

### Destination Ports

Use the Destination Ports table to indicate the forwarding or filtering action for frames received on the specified Receive port which are destined for the selected Source Address. Right-click on a port in the table, and select Forward, Block, Forward on All Ports, or Block on All Ports.

### Port

Displays the Destination port numbers.

### Current

Displays the current forwarding or filtering (blocking) action on the Destination port.

### Static

Displays the desired forwarding or filtering (blocking) action on the Destination port. Right-click in the table and select the desired action from the menu:

- **Forward** -- forward traffic out the Destination port to the Source Address entry.
- **Block** -- block traffic out the Destination port to the Source Address entry.

- **Forward on All Ports** -- forward traffic out all Destination ports to the Source Address entry.
- **Block on All Ports** -- block traffic out all Destination ports to the Source Address entry.

### Apply Button

Sets changes made in the Configure Address Filter area.

---

### Related Information

For information on related tasks:

- [How to Configure a Bridge Filtering Database](#)

## Bridge Spanning Tree Configuration Window

---

Use this window to view and modify the device's bridge port information relating to the Spanning Tree Algorithm (STA). The Spanning Tree Algorithm is the method that bridges use to ensure that only a single data route exists between any two end stations. Bridges use the STA to decide which is the controlling (root) bridge when two or more bridges are placed in parallel.

On a LAN (Local Area Network) interconnected by multiple bridges, Spanning Tree selects a controlling Root Bridge and Port for the entire bridged LAN, and a Designated Bridge and Port for each individual LAN segment. When traffic passes from one end station to another across the LAN, it is forwarded through the Designated Bridge/Port for the LAN segment, to the Root Bridge, which in turn forwards the traffic to the Designated Bridges/Ports on the opposite side. Bridges use Bridge Protocol Data Units (BPDUs) to communicate Spanning Tree information.

The Bridge Spanning Tree Configuration window displays STA parameters and allows you to alter parameters for the device bridge as a whole, and for each individual bridging interface.

To access the Bridge Spanning Tree Configuration window, select **Device > Bridge > Bridge Spanning Tree** from the Device View menu bar.

**Bridge Spanning Tree Configuration: 10.20.110.120**

Root		Configuration	
Bridge Address:	00-00-1D-73-82-E6	Root Bridge	Device
Cost To Bridge:	19	Protocol:	802.1 <input type="text" value="802.1"/>
Port Number:	19	Bridge Priority:	0x8000 <input type="text" value="8000"/>
Topology		Hello Time:	2 <input type="text" value="2"/>
The topology has changed 1045 times.		Max Age:	20 <input type="text" value="20"/>
Time Since Last Change: 0 Days 02:23:47		Forwarding Delay:	15 <input type="text" value="15"/>
		Hold Time:	1

Port	Priority	Path Cost	Designated Cost	Designated Root	Designated Bridge	Designated Port
1	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8001
2	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8002
3	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8003
4	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8004
5	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8005
6	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8006
7	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8007
8	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8008
9	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	8009
10	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	800A
11	0x80	19	19	00-00-1D-73-82-E6	00-E0-63-7E-04-A9	800B

Priority:  Path Cost:

Apply Close Refresh Help

Edit Mode.

## Root Area

### Bridge Address

Displays the physical (MAC) address of the bridge that is currently functioning as the Root Bridge.

### Cost to Bridge

Displays the cost of the data path from this device to the Root Bridge. Each port on each bridge adds a cost to a particular path that a frame must travel to the Root bridge. You can change the Path Cost of bridge ports using the [Path Cost field](#) in this window.

### Port Number

Displays the port number for the bridge port on this device that has the lowest cost path to the Root Bridge.

## *Topology Area*

### **Time Since Last Change**

Displays how many times the bridge topology has changed since power-up and the amount of time since the last change, in days hh:mm:ss format.

## *Configuration Area*

The fields in this area display values used for various Spanning Tree timers that are set at the Root Bridge and this device. The Spanning Tree operation uses the values set at the Root Bridge, but you can change the values for each bridge device on your network in the event it becomes root.

### **Root Bridge**

Displays the configuration parameters for the bridge that is currently root.

### **Device**

Displays the configuration parameters if this device becomes root.

### **Protocol**

Displays the Spanning Tree Algorithm (STA) Protocol Type the device is currently using: 802.1, DEC, or None. If the STA Protocol Type changed from None to either DEC or 802.1, restart the bridge in order to apply the newly-selected STA protocol.

### **Bridge Priority**

Displays the part of the bridge address, in hexadecimal format, that contains the value used in the Spanning Tree for priority comparisons. A lower value indicates a higher priority, and the bridge with the lowest value is selected as root. Allowable values range from 0 to FFFF hexadecimal (0 to 65535 decimal).

### **Hello Time**

Displays the length of time, in seconds, that the Root Bridge waits before re-sending configuration BPDUs. The range for this field is 1 to 10 seconds, with a default value of 2.

### **Max Age**

Displays the maximum time a BPDU can exist before it is discarded. Normally, each bridge in the network receives a new Configuration BPDU before the Max Age time is reached. If the time expires before a new BPDU is received, it indicates that the root is no longer active. The remaining bridges begin Spanning Tree operation to select a new root. The range for this field is 6 to 40 seconds, with a default value of 20 seconds.

### Forwarding Delay

The forwarding delay determines how long ports on the Root Bridge stay in each of the Listening and Learning states, when moving towards the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Filtering Database. The range for this field is 4 to 30 seconds, with a default value of 15 seconds.

### Hold Time

Displays the minimum time period, in seconds, that elapses between the transmission of Configuration BPDUs through a bridge port.

### *Bridge Port Table*

The following table displays information applicable to each bridge port on the device. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### Port

Displays the bridge port number.

### Priority

Displays the part of the port address that contains the identifier used in the Spanning Tree for priority comparisons. Allowable values range from 00 to FF hexadecimal (0 to 255 decimal). The default value is 80 hexadecimal. A lower assigned value gives the port a higher priority when BPDUs are compared.

---

**NOTE:** The X-Pedition Router supports only the values 01 to 0F hexadecimal (1 to 15 decimal).

---

### Path Cost

Displays the cost that the port contributes to the calculation of the overall cost of the path to the Root Bridge. You can lower a port's path cost to make the port more competitive in the selection of the Designated Port. For example, you may want to assign a lower path cost to a port on a higher performance bridge.

### Designated Cost

Displays the path cost to the Root Bridge from the Designated Port on the LAN segment to which this port is attached.

**Designated Root**

Displays the bridge identifier of the Root Bridge for this port.

**Designated Bridge**

Displays the bridge identifier of the Designated Bridge for this port.

**Designated Port**

Displays the port identifier for the port on the Designated Bridge that this port uses to communicate with the Root Bridge.

**Priority Field**

Use this field to change the [Priority](#) value for the port selected in the table above. Allowable values range from 00 to FF hexadecimal (0 to 255 decimal). The default value is 80 hexadecimal.

---

**NOTE:** The X-Pedition Router supports only the values 01 to 0F hexadecimal (1 to 15 decimal).

---

**Path Cost Field**

Use this field to change the [Path Cost](#) value for the port selected in the table above. The allowable range is 1 to 65535.

---

**Related Information**

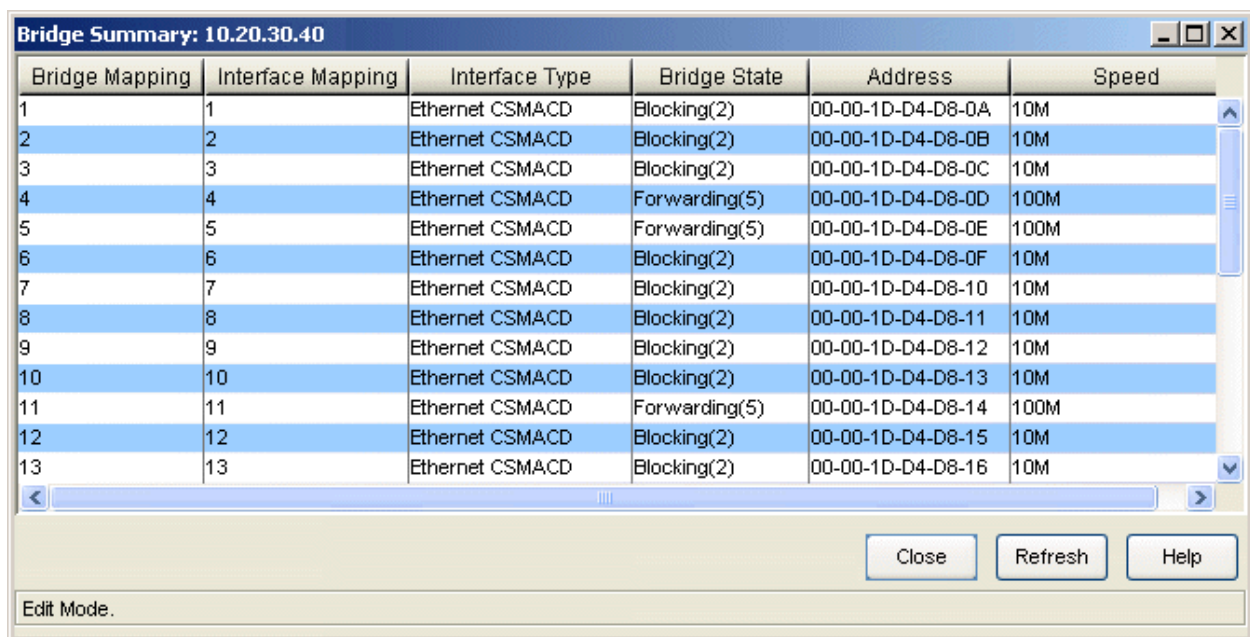
For information on related windows:

- [Bridge Filtering Database Window](#)
- [Bridge Summary Window](#)

## Bridge Summary Window

Use this window to view the current status of bridging across your device. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the Bridge Summary window, select **Device > Bridge > Bridge Summary** from the Device View menu bar.



The screenshot shows a window titled "Bridge Summary: 10.20.30.40". It contains a table with the following columns: Bridge Mapping, Interface Mapping, Interface Type, Bridge State, Address, and Speed. The table lists 13 rows of data. Below the table are buttons for "Close", "Refresh", and "Help". At the bottom left, it says "Edit Mode."

Bridge Mapping	Interface Mapping	Interface Type	Bridge State	Address	Speed
1	1	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-0A	10M
2	2	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-0B	10M
3	3	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-0C	10M
4	4	Ethernet CSMA/CD	Forwarding(5)	00-00-1D-D4-D8-0D	100M
5	5	Ethernet CSMA/CD	Forwarding(5)	00-00-1D-D4-D8-0E	100M
6	6	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-0F	10M
7	7	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-10	10M
8	8	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-11	10M
9	9	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-12	10M
10	10	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-13	10M
11	11	Ethernet CSMA/CD	Forwarding(5)	00-00-1D-D4-D8-14	100M
12	12	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-15	10M
13	13	Ethernet CSMA/CD	Blocking(2)	00-00-1D-D4-D8-16	10M

### Bridge Mapping

Displays the bridge port number of the port.

### Interface Mapping

Displays the interface number of the port.

### Interface Type

Displays the type of interface that applies to each bridge port.

### Bridge State

Displays the bridging state over the port interface:

- **Forwarding** -- Indicates that the port is on-line and configured to forward frames to and from its attached network.



- **Disabled** -- Indicates that no traffic can be received or forwarded (i.e., management disabled this port).
- **Listening** -- Indicates that this bridge port is not adding information to the Filtering Database. The port monitors Bridge Protocol Data Unit (BPDU) traffic while it prepares to move to the forwarding state.
- **Learning** -- Indicates that the port is monitoring network traffic and learning network addresses to create a Forwarding Database. This state may also mean that a network topology change caused the Spanning Tree Algorithm to be executed.
- **Blocking** -- Indicates that the port cannot receive or forward traffic. The Spanning Tree Algorithm configured this port to block (filter) frames to prevent redundant data loops in the bridged network.
- **Broken** -- Indicates that the port is unable to receive or forward traffic.
- **Unknown** -- Indicates that the bridging state over the port interface is unknown.

Right-clicking on a selected bridge port allows you to enable or disable the bridge state for that interface.

#### Address

Displays the physical address of the bridge port.

#### Speed

Displays an estimate of the interface bandwidth in bits per second. For an interface that either does not vary in bandwidth or where an accurate estimation cannot be made, this field displays the lowest bandwidth available.

---

### Related Information

For information on related windows:

- [Bridge Filtering Database Window](#)
- [Bridge Spanning Tree Configuration Window](#)
- [Find Source Address Window](#)

## Broadcast Suppression and Statistics Window

Use this window to monitor the number of broadcast packets received by each interface, and configure the number of broadcast packets forwarded to other interfaces. This feature helps to protect a network from broadcast storms.

To access the Broadcast Suppression and Statistics window, select **Device > Broadcast Suppression** from the Device View menu bar.

**Broadcast Suppression and Statistics: 10.20.30.40**

Current Broadcast Suppression Information:

IP Address	SlotId	Port	Total RX	Peak Rate	Time Since Peak	Threshold
10.20.30.40	2	1	0	0	0 Days 00:00:00	14880
10.20.30.40	2	2	0	0	0 Days 00:00:00	14880
10.20.30.40	2	3	0	0	0 Days 00:00:00	14880
10.20.30.40	2	4	0	0	0 Days 00:00:00	14880
10.20.30.40	2	5	0	0	0 Days 00:00:00	14880
10.20.30.40	2	6	0	0	0 Days 00:00:00	14880
10.20.30.40	2	7	0	0	0 Days 00:00:00	14880
10.20.30.40	2	8	0	0	0 Days 00:00:00	14880
10.20.30.40	2	9	0	0	0 Days 00:00:00	14880
10.20.30.40	2	10	0	0	0 Days 00:00:00	14880
10.20.30.40	2	11	0	0	0 Days 00:00:00	14880
10.20.30.40	2	12	0	0	0 Days 00:00:00	14880

Reset Peak Rate and Peak Time:

Receive Broadcast Threshold (Frames Per Second):

Edit Mode.

### *Current Broadcast Suppression Information*

Displays information about the broadcast packets received by each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

#### **IP Address**

The device's IP address.

**Slot ID**

The specific chassis slot where the port resides.

**Port**

The port number.

**Total RX**

Displays the total number of broadcast frames received on the selected port since the device was last initialized.

**Peak Rate**

Displays the peak rate (in frames per second) of broadcast frames received on the selected port since the device was last initialized or the peak value was last reset.

**Time Since Peak**

Displays the amount of time that has elapsed since the peak rate occurred.

**Threshold**

Displays the maximum number of received broadcast frames per second that may be forwarded by this interface to other interfaces on the device. Any number of broadcast frames above the selected threshold value are dropped.

**Reset Peak Rate and Peak Time**

Select **Yes** from this drop-down list to reset the peak rate and peak time values to zero.

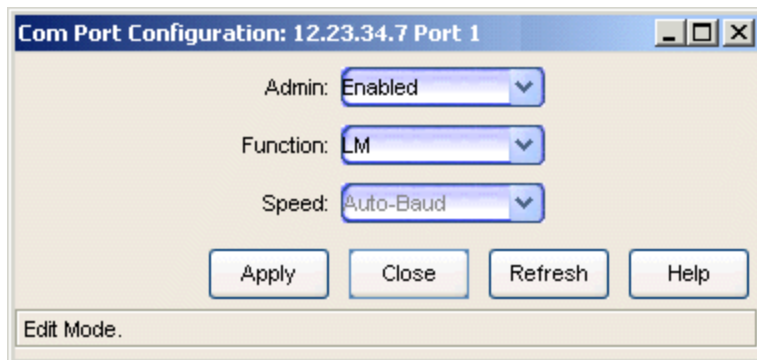
**Receive Broadcast Threshold (Frames Per Second)**

Use this field to change the threshold value for the selected port. This threshold sets the maximum number of received broadcast frames per second that may be forwarded by this interface to other interfaces on the device. Any number of broadcast frames above the threshold value are dropped. Select a port and enter the desired threshold value (in multiples of 10). Click **Apply** to set the new threshold value.

## Com Port Configuration Window

---

Use this window to configure a device's communications port(s). To access the Com Port Configuration window, select **Device > Configure Com Port 1** (or **Port 2** if applicable) from the Device View menu bar.



### Admin

Displays the administrative state of the selected communications port: **Enabled** or **Disabled**. Use the drop-down list to select the desired state.

### Function

Displays the functionality supported by the selected communications port:

- **LM** -- the port supports Local Management (LM).
- **UPS** -- the port supports an Uninterruptible Power Supply (UPS).
- **SLIP** -- the port supports the Serial Line Interconnect Protocol (SLIP). SLIP enables you to send TCP/IP packets across a serial line.
- **PPP** -- the port supports the Point-to-Point Protocol (PPP). PPP allows multi- protocol datagrams to be transmitted over a serial link.

Use the drop-down list to select the desired functionality.

### Speed

Displays the speed of the packets going over the selected communications port.

**NOTE:** This field is not configurable at this time.

## Configuration Upload/Download Window

---

To access the Configuration Upload/Download window from the main Console window, right-click the device in the left panel and select **Configuration Upload/Download** from the menu. In Device Manager, select **Utilities > Configuration Upload/Download** from the Device View menu bar.

---

**NOTE:** This window is only available for devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

---

*Sample Configuration Upload/Download window.*

*The fields displayed will vary depending on device type and MIB support.*

**Configuration Upload/Download: 10.20.30.40**

Current Device Settings

Active Image File:

Active Image Version:

Operation

Download Configuration File to Device

Upload Configuration File from Device

Upload Bootlog File from Device

Activate the Last Downloaded Configuration

Download Settings

TFTP Server IP:

Server uses Root Path:

Full Image Path:

Path to set on device:

Status

Operation Status:

Error Description:

Error Reason:

Bytes Transferred:

Current Values.

### *Current Device Settings*

The information displayed in Current Device Settings varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

**Active Image File**

Displays the location and filename of the active firmware image.

**Active Image Version**

Displays the firmware image currently active in the device.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

**Last Server IP**

Displays the IP address of the last TFTP server used.

**Last Filename**

Displays the path and filename of the last image downloaded to the device.

This is not necessarily the active firmware.

***etsysConfigurationManagementMIB* Devices that support** do not provide values for these fields and will display "No Information Provided".

*Operation*

The available operations vary depending on the device type. Use the radio buttons to select the desired type of operation:

- **Download Configuration File to Device** -- Performs a download of the specified configuration file to the device. On devices supporting the *ctDL* MIBs, the new configuration file will be activated following the download. Devices supporting the *cfgGroup* MIBs will require the separate [Activate the Last Downloaded Configuration](#) operation in order to activate the new configuration file.
- **Upload Configuration File from Device** -- Performs an upload of the device's active configuration file to the specified file on the TFTP server.
- **Upload Bootlog File from Device** -- Performs an upload of the device's bootlog to the specified file on the TFTP server. This option is only available for devices supporting the *cfgGroup* MIBs.
- **Activate the Last Downloaded Configuration** -- Activates the last downloaded configuration file. This option is only available for devices supporting the *cfgGroup* MIBs.

*Download Settings*

Use this area to specify the download settings.

**TFTP Server IP**

Enter the TFTP server's IP address, or use the dropdown list to select the TFTP server to perform the download or upload operation. The list displays

IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.

### Server Uses Root Path

If your TFTP server is configured with a root directory, select the checkbox and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to upload or download files to or from this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

### Full Image Path

Enter the full path and filename for the operation. You can also use the dropdown list to select the full path and filename, or use the **Browse** button to navigate to the file. For download operations, specify the name of the configuration file you want to download to the device. For upload operations, specify the name of the file where you want to store the uploaded configuration or bootlog file. (If you are creating a new file, browse to the directory and enter the new filename. The file will be created as part of the transfer operation.) The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a [Root Path](#), the browse capability is limited to the directories below that root path.

### Path to Set on Device

This field displays the target path and filename as it will be set on the device. If the [Server Uses Root Path](#) is selected, the specified root path is stripped from the full path and filename. If [Server uses Root Path](#) is not selected, this field displays the same path as the [Full Image Path](#) field.

### Status

The information displayed in Status varies depending on the device type.



---

**NOTE:** Devices that support *etsysConfigurationManagementMIB* will display dashes (--) in these fields until an operation begins, at which time they will report the progress of that operation.

---

### Operation Status

This field displays the status of the download operation, and varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

- **Idle** -- the device is currently not engaged in a transfer, and no error has occurred.
- **Sending** -- the device is uploading a configuration file or bootlog file to the server.
- **Receiving** -- the device is having a configuration file downloaded to it.
- **Transfer Complete** -- the transfer operation completed successfully
- **Error** -- an error occurred during the transfer. Refer to the [Error Description](#) and [Error Reason](#) fields for more information.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

- **Normal Operation** -- following a transfer, indicates that the operation was completed successfully. Also indicates the device is operating within normal parameters.
- **Download Active** -- the device is currently processing a TFTP download.
- **Error Detected During Download** -- a download was started but an error was detected. See the [Error Description field](#) for more information.
- **Other/Unknown** -- the device is in an unspecified or unknown state.

For devices that support *etsysConfigurationManagementMIB*, the information is displayed as follows:

- **Inactive** -- the device is currently not engaged in a transfer.
- **Pending** -- the transfer operation is in queue.
- **Running** -- the transfer operation is in progress.
- **Success** -- the transfer operation completed successfully.

- **Error Detected During Operation** -- an error occurred during the transfer. See the [Error Description field](#) for more information.

### Error Description

Displays a description of any error detected during a download. For devices that support the *cfgGroup* MIBs, it could be any of the following descriptions:

- **No Error** -- no errors were reported.
- **Timeout** -- a timeout error occurred.
- **Network Error** -- an error occurred on the network.
- **Device Memory Error** -- usually indicates the device's memory space is full.
- **Invalid Configuration** -- the downloaded configuration file was not valid for the device type.
- **Command Completed** -- the command issued to the device was completed successfully.
- **Internal Error** -- an error occurred on the device.
- **TFTP Server Error** -- an error occurred between the device and the server.

### Error Reason

Displays a reason for any error detected during a download. This field is only displayed for devices that support the *cfgGroup* MIBs.

### Bytes Transferred

Depending on the device and the TFTP server being used, this field may display transfer statistics during an operation. In some cases, a progress bar will also appear at the bottom of the screen (in the status bar), reporting the percentage of the transfer completed.

---

## Related Information

For information on related windows:

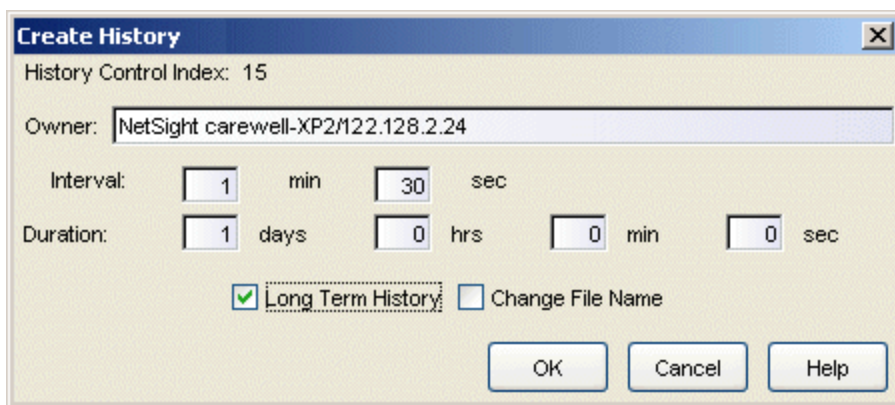
- [Firmware Image Download Window](#)

## Create/Modify History Window

---

Use this window to create your own RMON history tables or modify the parameters of existing history tables. Creating your own tables allows you to view statistical information collected at intervals other than those of the default tables (30 seconds and 30 minutes).

To modify an existing table, select the desired history table entry in the [RMON History List window](#), and click **Modify**. To create a new table, click **Create** in the RMON History List window. The Create/Modify History window opens.



### History Control Index

A number that uniquely identifies this history table.

### Owner

The owner, or originator, of the request to create the history table. Any request initiated by the RMON agent (i.e., the default host tables) shows its owner as monitor.

### Interval

Enter or modify the time interval between data collections. The time interval cannot exceed 60 minutes.

### Duration

Enter or modify the maximum range of time covered by the table. This time value defines the maximum number of entries that will be kept in the table before the oldest samples begin to be replaced by the newest ones. For example, a duration of one hour with an interval of 30 seconds would result in 120 entries.

### Long Term History

Use this checkbox to specify whether you want the history table data saved to a long term history .csv file. By default, long term history .csv files are stored in the *<install directory>*

\NetSight\jboss\server\default\deploy\NetSight\WebMonitor\Rmon directory with a default name comprised of the device IP number, the port interface, and the history index number.

### Change File Name

If this checkbox is selected, when you click **OK**, a file browser window opens where you can specify a file name and select a directory where the .csv file will be stored.

---

### Related Information

For information on related windows:

- [RMON History List Window](#)
- [RMON History Window](#)

## Ethernet Port Configuration Window

The Ethernet Port Configuration window displays the speed, duplex, flow control, and auto negotiation parameters for each port on the selected device. You can enable or disable auto negotiation for a selected port, and if auto negotiation is disabled, you can configure the port's speed, duplex, and flow control parameters. To access the Ethernet Port Configuration window, select **Device > Ethernet Port Configuration** from the Device View menu bar.

**Ethernet Port Configuration: 10.20.30.40**

Current Port Configuration Information:

IP Address	Port	Port Type	Link State	Remote Auto Signal	Auto Negotiate Configuration	Auto Negotiate Mode	Speed [Curre...
10.20.30.40	1	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	2	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	3	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	4	100Base-TX RJ45	Link	Detected	Complete	Enabled	100 Mbps
10.20.30.40	5	100Base-TX RJ45	Link	Detected	Complete	Enabled	100 Mbps
10.20.30.40	6	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	7	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	8	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	9	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	10	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	11	100Base-TX RJ45	Link	Detected	Complete	Enabled	100 Mbps
10.20.30.40	12	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	13	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	14	100Base-TX RJ45	No Link	Not Detected	Configuring	Enabled	Unknown
10.20.30.40	15	100Base-TX RJ45	Link	Detected	Complete	Enabled	100 Mbps

Auto Negotiate Technology:

Advertised	Local	Remote	Operational Modes
Enabled	Yes	No	10 Base-T Half Duplex
Enabled	Yes	No	10 Base-T Full Duplex
---	No	No	100 Base-T4 Half Duplex
Enabled	Yes	No	100 Base-TX Half Duplex
Enabled	Yes	No	100 Base-TX Full Duplex
Enabled	Yes	No	Full Duplex Flow Control
---	No	No	Full Duplex Asymmetric Flow Co...
---	No	No	Full Duplex Symmetric Flow Cont...
---	No	No	Full Duplex Asymmetric and Sym...

Configure Parameters:

	Current	Manual
Auto Negotiate Config:	Configuring	Enabled
Speed:	Unknown	10 Mbps
Duplex:	Unknown	Half Duplex
Flow Control:	Enabled	Enabled

Buttons: Apply, Close, Refresh, Help

Edit Mode.

### Current Port Configuration Information Table

This table displays the current configuration information for all the ports on the device. Select a port to display and configure its parameters in the bottom portion of the window. If you select multiple ports (using the **Shift** or **Ctrl** keys), the information for first port selected will be displayed below, however any changes you make will be applied to all the selected ports. Console provides

table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**IP Address**

The IP address of the device.

**Port**

The port number.

**Port Type**

The type of port.

**Link State**

Defines the status of the port's connection (link) with a remote port: **Link** or **No Link**.

**Remote Auto Signal**

Indicates whether auto negotiation signaling is detected on the remote port: **Detected** or **Not Detected**.

**Auto Negotiate Configuration**

Indicates whether auto negotiation signaling is in progress (**Configuring**) or has completed (**Complete**).

**Auto Negotiate Mode**

Displays whether auto negotiation is enabled or disabled on the port.

**Speed (Current)**

Displays the currently supported speed for the port.

**Speed (Manual)**

Displays the configured speed for the port when it is not set to auto negotiation.

**Duplex Mode (Current)**

Displays the current duplex mode for the port: **Half Duplex** or **Full Duplex**.

**Duplex Mode (Manual)**

Displays the duplex mode for the port when it is not set to auto negotiation: **Half Duplex** or **Full Duplex**.

**Flow Control (Current)**

Displays the current [flow control method](#) for the port.

### Flow Control (Manual)

Displays the [flow control method](#) for the port when it is not set to auto negotiation.

### *Operational Mode (Advertised)*

Indicates the local port's advertised ability for each specific operational mode. The advertised ability only becomes active on ports that have auto negotiation enabled.

### *Operational Mode (Local)*

Indicates whether the local port's hardware capability supports each specific operational mode.

### *Operational Mode (Remote)*

Indicates the remote port's advertised ability for each specific operational mode.

## *Configure Parameters*

Use this section to enable or disable auto negotiation for a selected port or ports. If auto negotiation is disabled, you can manually configure the speed, duplex, and flow control parameters of the selected port(s).

---

**NOTE:** To configure parameters on multiple ports, select the ports in the table above using the **Ctrl** or **Shift** keys. The information for first port selected will be displayed here, however any changes you make will be applied to all the selected ports.

---

The Current column displays the currently configured parameters for the selected port. If auto negotiation is enabled, the column displays the mode negotiated with the remote port. If auto negotiation is disabled, the column displays the modes manually configured on the port. Use the drop-down lists in the Manual column to manually configure the parameters when auto negotiation is disabled on the port.

---

**NOTE:** If you manually configure these parameters, be sure that the remote port supports the same mode. Otherwise, no link between the local and remote port will be achieved.

---

### Auto Negotiate Config

Displays the current status of auto negotiation signaling on the selected port. Use the drop-down list to **Enable** or **Disable** auto negotiation.

### Speed

Displays the current speed of the selected port. Use the drop-down list to select the speed if auto negotiation is disabled on the port.

### Duplex

Displays the current duplex mode for the selected port. Use the drop-down list to select the mode if auto negotiation is disabled on the port.

### Flow Control

Displays the current flow control method that the selected port uses to notify the remote port that congestion is occurring and that the sending device should stop transmitting until the congestion can be cleared.

Available options vary based on the port's duplex mode.

- **Symmetric**-- Indicates that the port is able to both receive and transmit pause control frames.
- **Asymmetric RX** -- Indicates that the port can receive pause control frames, but does not transmit its own. This option is only available for Gigabit Ethernet ports.
- **Asymmetric TX** -- Indicates that the port can send pause control frames, but does not acknowledge received pause control frames. This option is only available for Gigabit Ethernet ports.
- **Auto Negotiate** -- Indicates that the port only uses pause control frames if the negotiation process determines that the remote port supports them. Both ends of the link must support auto negotiation and a common mode of operation.
- **Enabled** -- Indicates that flow control is enabled on the port.
- **Disabled** -- Indicates that flow control is disabled on the port.

### *Auto Negotiate Technology Area*

This section displays which operational modes are supported by the local and remote ports, and which modes that are supported by the local port are being advertised to the remote port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see .

---

**NOTE:** This section does not apply if you have manually configured specific operational modes for your 100Base-TX port, or if you are configuring a 100Base-FX port.

---



### Advertised

Displays whether an operational mode is advertised to the remote port. Only those modes supported by the local port can be advertised.

- **Enabled** -- Indicates that the mode is supported and is being advertised.
- **Disabled** -- Indicates that the mode is supported but is not being advertised.
- --- Indicates that the mode is not supported.

You can change whether a supported mode is advertised by the port by right-clicking on the supported mode and selecting **Enable** or **Disable**. You can enable or disable all supported modes by right-clicking on any mode and selecting **All Enable** or **All Disable**.

---

**NOTE:** If you have selected multiple ports in the table above, this section displays the information for first port selected, however any changes you make will be applied to all the selected ports.

---

### Local

Displays whether the operational mode is supported by the local port: **Yes** or **No**.

### Remote

Displays whether the operational mode is supported by the remote port: **Yes** or **No**.

### Operational Modes

Lists the possible operational modes (e.g., Full Duplex Flow Control, 10Base-T Half Duplex, Full Duplex Symmetric Flow Control, etc.).

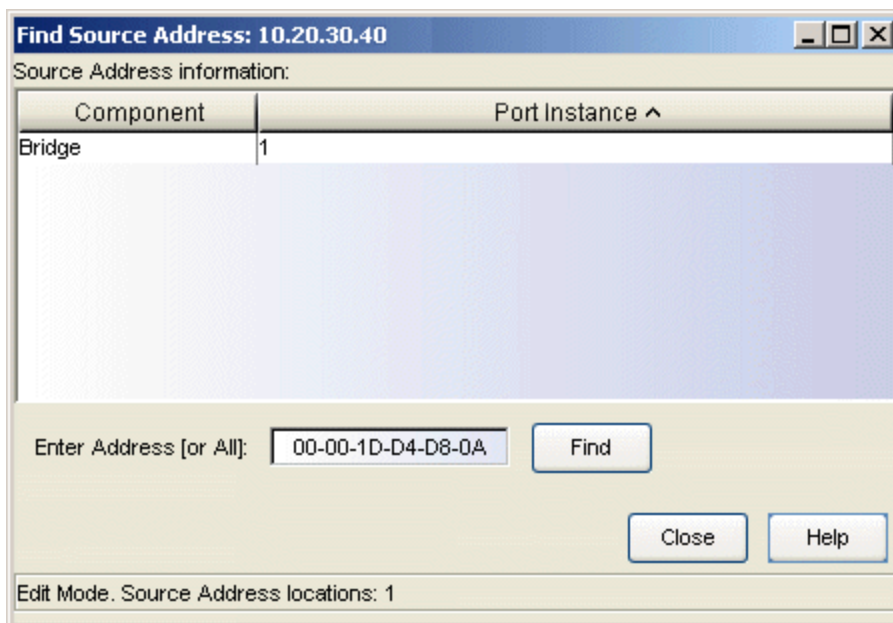
## Find Source Address Window

---

Use the Find Source Address window to locate the source port for a specific MAC address on the selected device. When you perform a Find operation, the device's Filtering Database is searched for the specified MAC address. If it is found, the Component field will display the value "Bridge" indicating that the address was found on a bridging interface. The Port Instance field will display the index number assigned to the bridge port on which the address was located.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the Find Source Address window, select **Device > Bridge > Find Source Address** from the Device View menu bar.



### Component

Displays the type of interface through which the specified MAC address is communicating. This field will report Bridge. You can sort the entries by clicking on the column heading.

**Port Instance**

Displays the bridge port index number on which the specified MAC address was found. Bridge port index numbers may not match interface port index numbers (the MIB-II *ifIndex* value) because there is an offset in the mapping between the two. Use a MIB tool to query *dot1dBasePortIfIndex*(1.3.6.1.2.1.17.1.4.1.2) and view the mapping and offset. You can sort the entries by clicking on the column heading

**Enter Address (or All)**

Enter the source address you want to find, in XX-XX-XX-XX-XX-XX format. If you enter All, the Port Instance for every entry in the device's Filtering Database will be displayed.

---

**Related Information**

For information on related tasks:

- [How to Find a Source Address](#)

## Firmware Image Download Window

---

This window enables you to download a firmware image file to a device. You must have a TFTP Server running to perform the download operation. To access the Firmware Image Download window from the main Console window, right-click the device in the left panel and select **Firmware Image Download** from the menu. In Device Manager, select **Utilities > Firmware Image Download** from the Device View menu bar.

---

**NOTE:** This window is only available for devices that support the *etsysConfigurationManagementMIB*, *cfgGroup*, or *ctDL* MIBs.

---

**Firmware Image Download: 10.20.30.40**

Current Device Settings

Last Server IP: 10.20.31.51

Last Filename: \\firmware\6000\50305.FLS

Operation

Download

Download & Reset

Reset

Download Settings

TFTP Server IP: 124.121.192.52 (local)

Server uses Root Path: C:\tftpboot

Full Image Path: \\firmware\6000\50305.FLS (current)

Path to set on device: \\firmware\6000\50305.FLS

Status

Operation Status: Normal Operation

Error Description:

Bytes Transferred:

Current Values.

### *Current Device Settings*

The information displayed in Current Device Settings varies depending on the device type.

For devices that support the *cfgGroup* MIBs (such as the X-Pedition Router), the information is displayed as follows:

#### **Active Image File**

Displays the location and filename of the active firmware image.

**Active Image Version**

Displays the firmware image currently active in the device.

For devices that support the *ctDL* MIBs, the information is displayed as follows:

**Last Server IP**

Displays the IP address of the last TFTP server used.

**Last Filename**

Displays the path and filename of the last image downloaded to the device.  
This is not necessarily the active firmware.

Devices that support *etsysConfigurationManagementMIB* do not provide values for these fields and will display "No Information Provided".

*Operation*

Use the radio buttons to select the desired type of operation:

- **Download** -- Performs a download of the specified firmware image to the device. This operation will not activate the new firmware. A Reset operation must be performed to activate the downloaded image.
- **Download & Reset** -- Performs a download of the specified firmware image to the device and resets the device with the new image as soon as the download is complete.
- **Reset** -- Resets the device so that new firmware can be activated.

*Download Settings*

Use this area to specify the download settings.

**TFTP Server IP**

Enter the TFTP server's IP address, or use the dropdown list to select the TFTP server to perform the download operation. The list displays IP addresses for the local workstation (local), the TFTP server last set on the device (current), and the last 3-5 TFTP servers used in this window.

**Server Uses Root Path**

If your TFTP server is configured with a root directory, select the checkbox and specify the root directory in the Path field (or use the **Browse** button to navigate to the directory). The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to download files from this directory and any of its sub-directories. If the NetSight TFTP Service is being used, the checkbox will be selected with the root path as specified in the Services for NetSight Server view of the

Options window.

---

**NOTES:** Devices that support *etsysConfigurationManagementMIB* **must** use a TFTP server that is configured with a root directory.

When using a remote TFTP server, mount or map the remote machine's TFTP root directory. Then specify the mounted or mapped drive as the root directory.

---

### Full Image Path

Enter the full path and filename of the image file you want to download to the device. You can also use the dropdown list to select a path and filename or use the **Browse** button to navigate to the file. The dropdown list displays the path as set on the device (current), and the last five paths used in this window. If you have specified a [Root Path](#), the browse capability is limited to the directories below that root path.

### Path to Set on Device

This field displays the image path as it will be set on the device. If the [Server Uses Root Path](#) is selected, the specified root path is stripped from the full path and filename. If [Server uses Root Path](#) is not selected, this field displays the same path as the [Full Image Path](#) field.

### Status

The information displayed in Status varies depending on the device type.

---

**NOTE:** Devices that support *etsysConfigurationManagementMIB* will display dashes (--) in these fields until an operation begins, at which time they will report the progress of that operation.

---

### Operation Status

Displays the status of the download operation:

- **Normal Operation** -- following a download, indicates that the operation was completed successfully. Also indicates the device is operating within normal parameters.
  - **Download Active** -- the device is currently processing a TFTP download.
  - **Error Detected During Download** -- a download was started but an error was detected.
  - **Other/Unknown** -- the device is in an unspecified or unknown state.
- For devices that support *etsysConfigurationManagementMIB*, the

information is displayed as follows:

- **Inactive** -- the device is currently not engaged in a transfer.
- **Pending** -- the transfer operation is in queue.
- **Running** -- the transfer operation is in progress.
- **Success** -- the transfer operation completed successfully.
- **Error Detected During Operation** -- an error occurred during the transfer.

#### **Error Description**

Displays a description of any error detected during a download.

#### **Bytes Transferred**

Depending on the device and the TFTP server being used, this field may display transfer statistics during a download operation. In some cases, a progress bar will also appear at the bottom of the screen (in the status bar), reporting the percentage of the download operation completed.

---

#### **Related Information**

For information on related windows:

- [Configuration Upload/Download Window](#)



## ICMP Group Window

Use the ICMP (Internet Control Message Protocol) Group window to display statistics that reflect the operating status of the Internet layer. The window displays the number and type of ICMP messages received and transmitted by the device.

To access the ICMP Group window, select **Device > MIB-II > ICMP Group** from the Device View menu bar.

	Received	Transmitted
Total Messages:	2309	2328
Errors:	0	0
Destination Unreachable:	2	21
Time Exceeded:	0	0
Parameter Problem:	0	0
SourceQuench:	0	0
Redirect:	0	0
Echo Request:	2307	0
Echo Reply:	0	2307
Timestamp Request:	0	0
Timestamp Reply:	0	0
Address Mask Request:	0	0
Address Mask Reply:	0	0

Close Refresh Help

Current Values.

### Total Messages

Displays the total number of ICMP messages that the device received and transmitted (including error messages).

### Errors

Displays the number of ICMP messages that the device received and transmitted but had ICMP-specific errors: bad ICMP checksums, bad length, etc.

**Destination Unreachable**

Displays the number of ICMP Destination Unreachable messages received and transmitted by the device. A gateway issues a destination unreachable message when it cannot deliver a datagram due to one of the following problems:

- Network, host, protocol, or port was unreachable.
- Fragmentation was necessary, but disallowed by the Do Not Fragment bit.
- Source route failed.
- Destination network or host is unknown.
- Source host is isolated.
- Communication with the destination network or host is administratively prohibited.
- Network or host is unreachable for the type of service.

**Time Exceeded**

Displays the number of ICMP Time Exceeded messages received and transmitted. A router sends a Time Exceeded message to the device that transmitted the original datagram when it discards it either because the Time To Live counter (also known as the Hop Count) reached zero or because the reassembly counter expired while waiting for fragments. Time Exceeded messages can indicate either an excessively long route from source to destination or a circular route due to errors in the routing tables.

**Parameter Problem**

Displays the number of ICMP Parameter Problem messages received and transmitted. A Parameter Problem message indicates that a datagram was discarded due to a problem not covered by any of the previous messages.

**SourceQuench**

Displays the number of ICMP Source Quench messages received and transmitted. A router issues a Source Quench message when network traffic overwhelms the buffering capacity of the router. It instructs a host to slow its current rate of datagram transmission.

**Redirect**

Displays the number of ICMP Redirect messages received and transmitted. When a host transmits, it uses minimal routing information. It learns new routes from routers. A router that detects a host using an inefficient route sends a redirect message that contains new routing information.

**Echo Request**

Displays the number of ICMP Echo (request) messages received and transmitted. Echo messages are used to test connectivity between two network devices.

**Echo Reply**

Displays the number of ICMP Echo Reply messages received and transmitted. Echo messages are used to test connectivity between two network devices.

**Timestamp Request**

Displays the number of ICMP Timestamp Request messages received. To synchronize system clocks, a device issues a timestamp request to another network device. The destination device then issues a timestamp reply message that includes the system time.

**Timestamp Reply**

Displays the number of ICMP Timestamp Reply messages received and transmitted. To synchronize system clocks, a device issues a timestamp request to another network device. The destination device then issues a timestamp reply message that includes the system time.

**Address Mask Request**

Displays the number of ICMP Address Mask Request messages received and transmitted. To determine the network subnet mask, a device issues an address mask request, either targeted to a specific address or as a broadcast to the entire network. The responding device includes the network subnet mask in an address mask reply.

**Address Mask Reply**

Displays the number of ICMP Address Mask Reply messages received and transmitted. To determine the network subnet mask, a device issues an address mask request, either targeted to a specific address or as a broadcast to the entire network. The responding device includes the network subnet mask in an address mask reply.

---

**Related Information**

For information on related windows:

- [System Group Window](#)
- [SNMP Group Window](#)

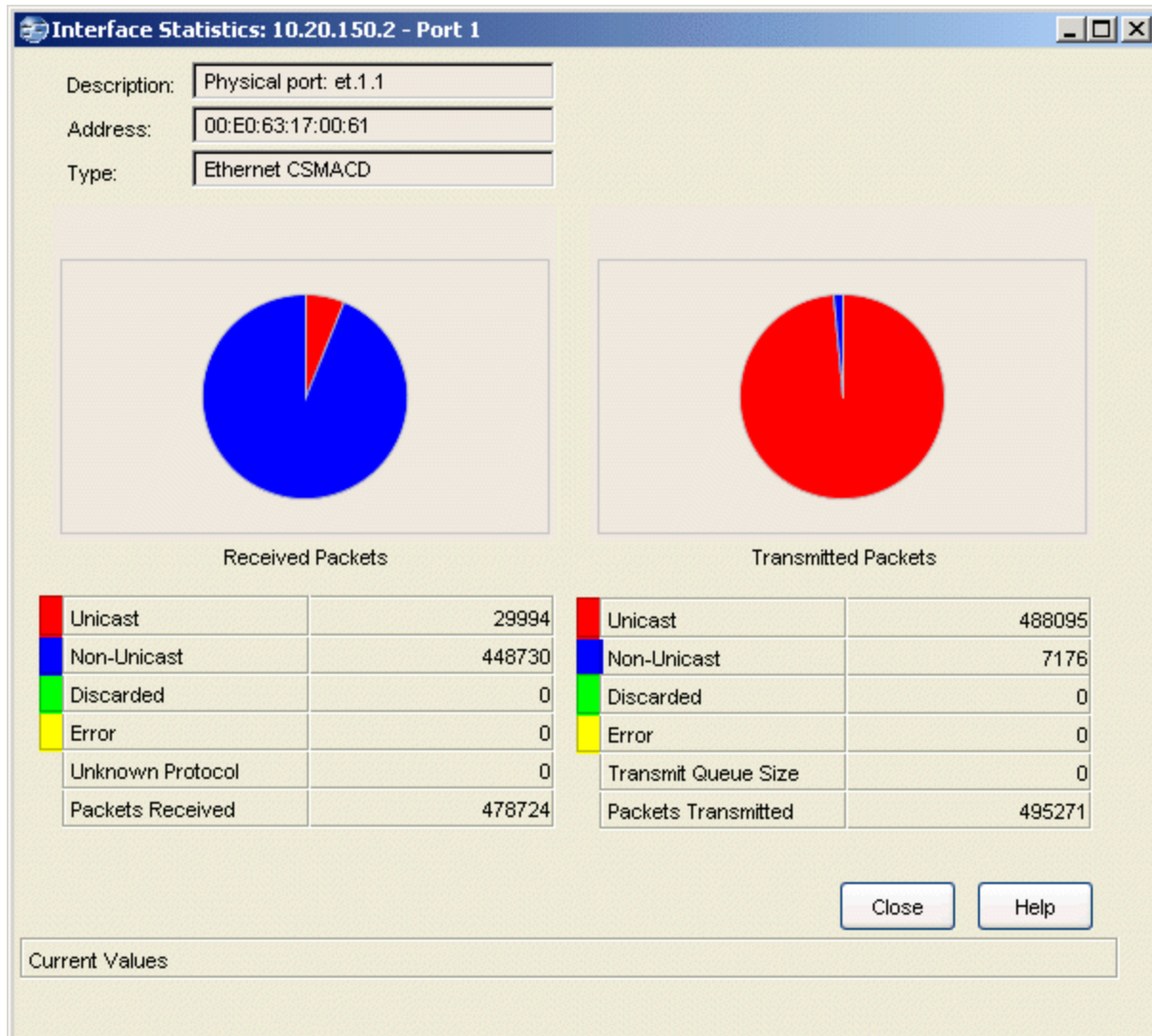
## Interface Statistics Window

---

Use this window to view color-coded statistical information about each individual bridge port on your device. The first four statistics are graphically displayed in color-coded form in the pie chart. These statistics are updated with each poll to the device.

To access the Interface Statistics window from Device Manager, click on the desired port number in the Device View and select **Interface Statistics** from the port menu. To access this window from Console, select the desired port in the Port View of the Properties tab or in a FlexView table, and use the right-click menu option.

This window can also be accessed from the [Interface Summary](#) window by selecting the desired interface, and clicking on **Statistics**.

**Description**

Displays a description of the port and the type of interface followed by the board and port number.

**Address**

Displays the physical address of the selected port.

**Type**

Displays the type of interface.

**Pie Chart**

Displays interface statistics in a graphical pie-chart format.

**Received Packets**

Displays the type and number of packets received by the interface.

**Transmitted Packets**

Displays the type and number of packets transmitted by the interface.

**Unicast**

Displays the number of packets received/transmitted by the interface that had a single, unique source or destination address.

**Non-Unicast**

Displays the number of packets received/transmitted by the interface that had a source or destination address recognized by more than one device on the network segment. This field includes a count of broadcast packets -- those recognized by all devices on a segment.

**Discarded**

Displays the number of packets received/transmitted by the interface that were discarded, even though no errors were detected. If good packets are discarded, a busy network must need to free up buffer space. This usually means that network traffic is overwhelming the device.

**Error**

Displays the number of received/transmitted packets that contained errors.

**Unknown Protocol**

Displays the number of received packets that were discarded because of an unknown or unsupported protocol.

**Transmit Queue Size**

Displays the length of the output packet queue, in packets. The availability of device buffer space and the level of traffic on the target network determine how large the output packet queue can grow before the device begins to discard packets.

**Packets Received**

Displays the total number of packets received by the interface.

**Packets Transmitted**

Displays the total number of packets transmitted by the interface.

---

**Related Information**

For information on related windows:

- [Interface Summary Window](#)

## Interface Summary Window

Use this window to view information about each port interface on the device, and to also access a detailed Interface Statistics window for each interface listed.

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the Interface Summary window, select **Device > MIB-II > Interface Summary** from the Device View menu bar.

Interface	Type	Description	Physical Status	Logical Status	Address	Speed
1	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
2	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
3	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
4	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Up	Up	00-00-1D-D4-D8...	100M
5	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Up	Up	00-00-1D-D4-D8...	100M
6	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
7	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
8	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
9	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
10	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
11	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Up	Up	00-00-1D-D4-D8...	100M
12	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
13	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
14	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
15	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Up	Up	00-00-1D-D4-D8...	100M
16	Ethernet CSMA/CD	Fast Ethernet Frontpanel	Down	Up	00-00-1D-D4-D8...	10M
17	Ethernet CSMA/CD	Gigabit Ethernet Port	Up	Up	00-00-1D-D4-D8...	1G
18	Ethernet CSMA/CD	FTM Backplane Port 1	Up	Up	00-00-1D-D4-D8...	800M
19	Ethernet CSMA/CD	FTM Backplane Port 3	Up	Up	00-00-1D-D4-D8...	800M
20	Ethernet CSMA/CD	FTM Backplane Port 4	Up	Up	00-00-1D-D4-D8...	800M

### Interface

Displays the index value assigned to each port interface on the device.

### Type

Displays the type of port interface.

### Description

Displays a description of the port and the type of interface followed by the board and port number.

### Physical Status

Displays the current operational state of the port interface:

- **On** -- the operational status is up
- **Off** -- the operational status is down
- **Dormant** -- the interface is waiting for external actions (such as a serial line waiting for an incoming connection)
- **Lower Layer Down** -- the interface is down due to the state of lower-layer interface(s)
- **Not Present** -- the interface has missing components (usually hardware)
- **Testing** -- operational status testing; no operational packets can be passed
- **Unknown** -- the device is returning the value Unknown or a value that the software does not recognize

### Logical Status

Displays the current administrative state of the port interface: Up or Down.

### Address

Displays the physical (MAC) address of the port interface.

### Speed

Displays an estimate of the interface bandwidth in bits per second. For an interface that either does not vary in bandwidth or where an accurate estimation cannot be made, this field displays the lowest bandwidth available.

### Statistics Button

Select the desired interface, and click **Statistics** to access the [Interface Statistics](#) window.

---

### Related Information

For information on related windows:

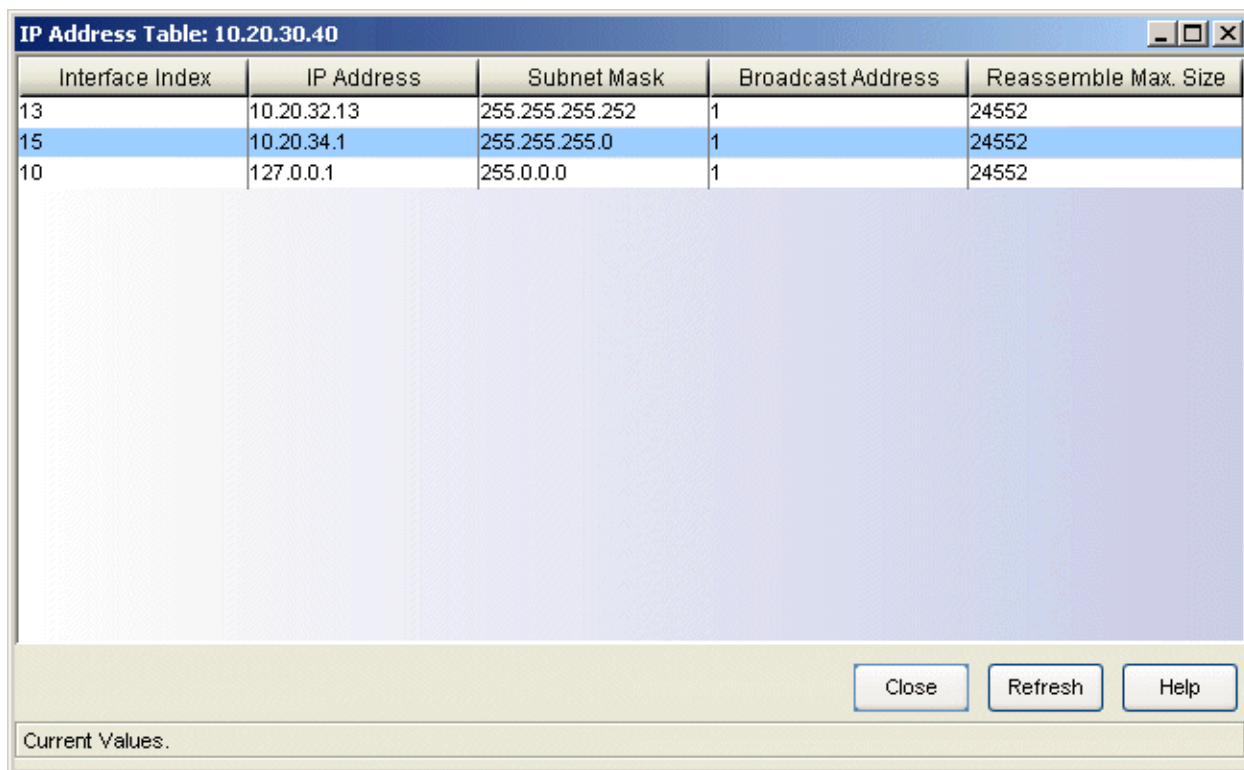
- [Interface Statistics Window](#)



## IP Address Table Window

Use this window to verify port broadcast addresses, and reassembly guidelines for fragments. This window also displays IP addresses and subnet masks for ports on the device. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the IP Address Table window, select **Device > MIB-II > IP Address Table** from the Device View menu bar.



Interface Index	IP Address	Subnet Mask	Broadcast Address	Reassemble Max. Size
13	10.20.32.13	255.255.255.252	1	24552
15	10.20.34.1	255.255.255.0	1	24552
10	127.0.0.1	255.0.0.0	1	24552

Close Refresh Help

Current Values.

### Interface Index

The index value which uniquely identifies the interface.

### IP Address

The IP address for the interface.

### Subnet Mask

Displays the subnet mask associated with the IP address of this entry.

**Broadcast Address**

Displays the value of the least significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. This field determines whether 1s or 0s are used to address IP packets that are sent as network broadcasts.

**Reassemble Max. Size**

Displays the size of the largest IP datagram that the device can reassemble from fragmented datagrams received through this interface. The maximum size of a complete IP datagram is 65,535 bits.

---

**Related Information**

For information on related windows:

- [IP Group Window](#)

## IP Group Window

Use this window to view a statistical breakdown of the number of datagrams received by and transmitted from the device. This window also counts the various types of fragmented and reassembled datagrams.

To access the IP Group window, select **Device > MIB-II > IP Group** from the Device View menu bar.

Received Datagrams	
Total:	90765
Header Errors:	0
Address Errors:	0
Forwarded:	0
Unknown Protocol:	0
Discarded:	0
Delivered:	90765

Datagram Fragments	
Datagrams Fragmented:	0
Fragments Discarded:	0
Fragments Created:	0

Datagrams Reassembly	
Fragments Received:	0
Datagrams Reassembled:	0
Reassembly Failures:	0
ReassemblyTimeout:	1

Transmitted Datagrams	
Total:	90705
Discarded:	0
No Route:	0

Forwarding State: Host  
Time To Live: 255

Buttons: Apply, Close, Refresh, Help

Current Values.

### *Received Datagrams Area*

Displays the type and number of datagrams received from interfaces.

#### **Total**

Displays the total number of datagrams received from interfaces, including those received in error.

#### **Header Errors**

Displays the number of received datagrams discarded due to errors in their IP headers: bad checksums, version number mismatches, format errors,

time-to-live exceeded, etc. (When a device receives an IP datagram, it checks the header for errors.)

**Address Errors**

Displays the number of received datagrams discarded when the IP address in the destination field of the header is invalid (to be received at this device). This count also includes invalid addresses and addresses of unsupported classes. If the device is not a gateway, this counter also includes datagrams discarded when the destination address is not local.

**Forwarded**

Displays the number of received datagrams which have not found their final destination (at this device) when attempts were made to find an alternative route. For devices that do not function as gateways, this counter also includes those packets which were successfully source-routed via this device.

**Unknown Protocol**

Displays the number of locally-addressed datagrams that were received but were discarded because of an unknown or unsupported protocol.

**Discarded**

Displays the number of received datagrams that were discarded even though no problems were encountered to prevent their continued processing. This counter does not include any datagrams discarded while waiting for reassembly.

**Delivered**

Displays the number of received datagrams delivered to IP user-protocols.

***Transmitted Datagrams Area***

Displays the type and number of datagrams that local IP user-protocols supplied to IP in requests for transmission.

**Total**

Displays the total number of IP datagrams that local IP user-protocols supplied to IP in requests for transmission.

**Discarded**

Displays the number of transmitted datagrams that were discarded even though no problems were encountered.

**No Route**

Displays the number of IP datagrams discarded because no route could be found to transmit them to their destination.

***Datagram Fragments Area***

Displays the number of fragmented datagrams created or discarded by the interface.

**Datagrams Fragmented**

Displays the number of datagrams that were fragmented because they exceeded the maximum size for the transmission media field.

**Fragments Discarded**

Displays the number of datagrams discarded because the flag field in the datagram did not permit fragmentation.

**Fragments Created**

Displays the number of IP datagram fragments generated as a result of fragmentation at this device.

***Datagrams Reassembly Area***

Displays information about fragments received from the network and the status of reassembly attempts.

**Fragments Received**

Displays the number of IP fragments received from the network.

**Datagrams Reassembled**

Displays the number of IP datagrams reassembled.

**Reassembly Failures**

Displays the number of failures detected by the IP reassemble algorithm (e.g., timed out, errors, etc.).

**Reassembly Timeout**

Displays the maximum number of seconds that received fragments are held while they wait for reassembly at this device.

**Forwarding State**

Determines whether this device functions as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this device. By enabling or disabling IP Forwarding, you enable or disable the ability of the device to route IP datagrams. There are two possible states:

- **Gateway** -- Device forwards datagrams.
- **Host** -- Device does not forward datagrams (except those datagrams source-routed via the host).

### Time to Live

Displays the number of seconds a datagram can continue to exist on the network. You can enter a new value; allowable values range from **1** to **255** seconds. Any datagram that exceeds this limit is discarded.

---

### Related Information

For information on related windows:

- [System Group Window](#)
- [SNMP Group Window](#)

## MIB Information Window

---

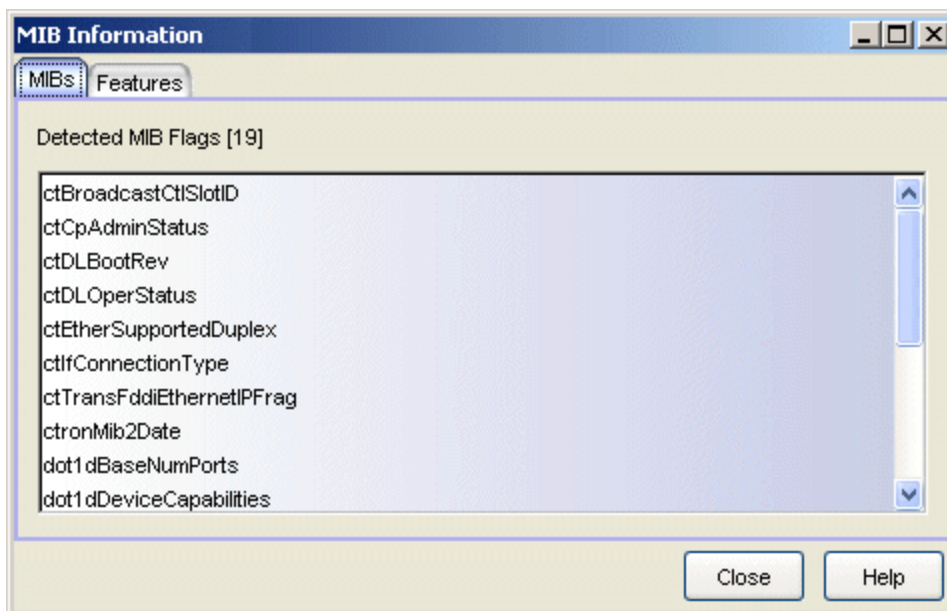
The MIB Information window provides information that is useful when troubleshooting Device Manager functionality. The window displays two tabs that provide information on the device's MIBs and features. To access the MIB Information window, select **Help > MIB Information** from the Device View menu bar.

Information on the following tabs:

- [MIBs](#)
- [Features](#)

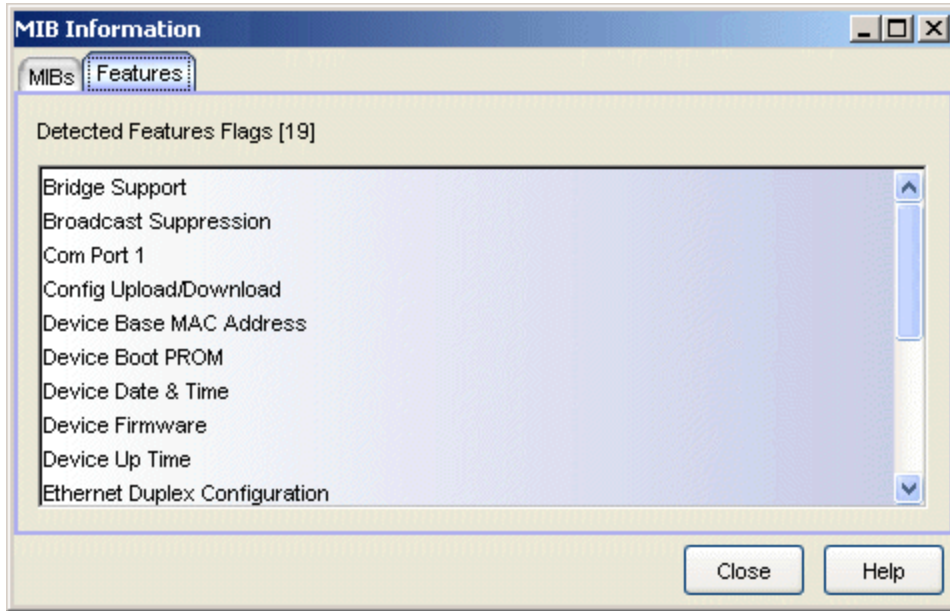
### *MIBs Tab*

The MIBs tabbed page displays the detected MIBs (Management Information Bases) on the device currently being monitored. Network devices draw their functionality from a collection of MIBs. The MIBs tab displays those MIBs, and therefore the functionality supported by the device.



### *Features Tab*

The Features tabbed page displays the detected features on the device currently being monitored.

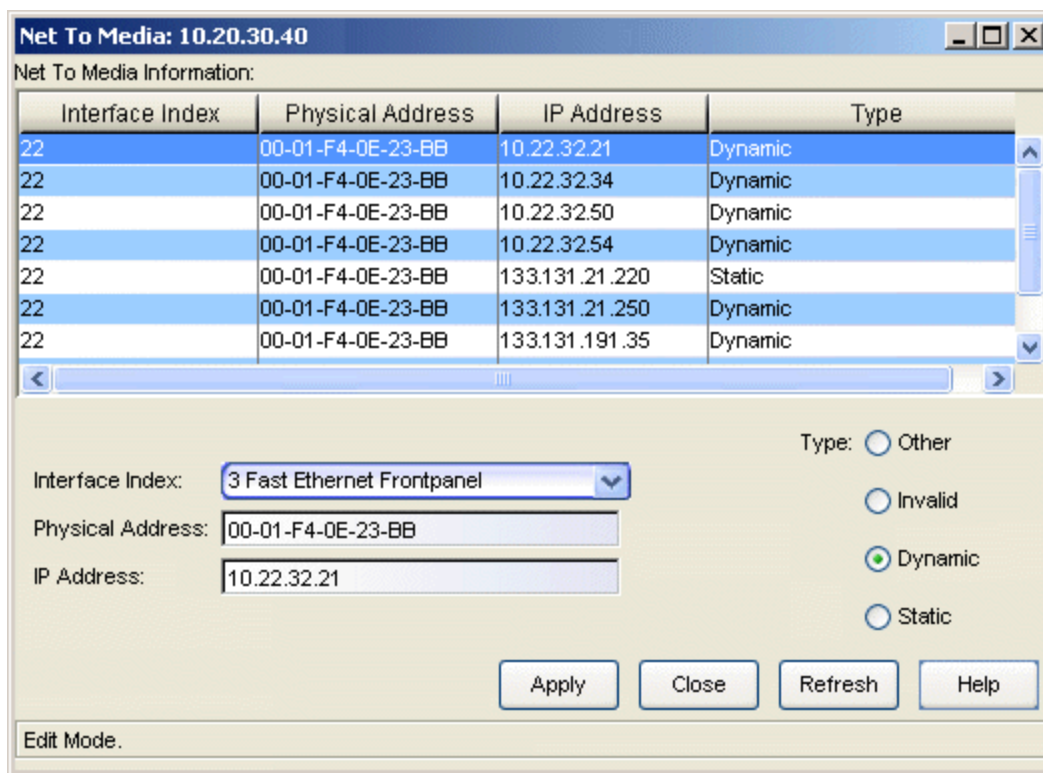




## Net To Media Window

Use this window to map IP addresses into physical addresses. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the Net To Media window, select **Device > MIB-II > Net To Media** from the Device View menu bar.



### Interface Index

The index value which uniquely identifies the interface.

### Physical Address

Displays the physical interface address of the device.

### IP Address

Displays the IP address corresponding to the media-dependent physical address for that entry.

## Type

Displays the media types that can be used to map an entry in the table:

- **Dynamic** -- Indicates that entries are added to the acquired database through the learning process.
- **Static** -- Indicates that an entry is added to the permanent database.
- **Invalid** -- Indicates that an invalid mapping occurred. An invalid entry may (or may not) be deleted from the Net To Media Table, depending on how that device handles invalid mapping types.
- **Other** -- Indicates that none of the above are true.

## Interface Index Field

Use this drop-down list to select an [interface index](#). The list displays a description of the network interface on which this device sends and receives IP datagrams.

## Physical Address Field

Use this field to enter the [physical address](#) of the selected interface.

## IP Address Field

Use this field to enter the [IP address](#) of the selected interface.

## Type Selection

Select the desired [type](#) option for the selected interface.

---

## Related Information

For information on related windows:

- [IP Group Window](#)

## RMON Alarm/Event List

---

Although Alarms and Events are defined as separate RMON features, neither one can function properly without the other. You can define an alarm threshold, but if it doesn't point to an event, there will be no indication that the threshold has been crossed. Similarly, you can define an event, but unless it is attached to an alarm threshold, it won't be triggered. Each is an essential part of the same notification process: the alarm defines a set of conditions you want to know about, and the event provides the means of letting you know those conditions have occurred.

Console's RMON Alarm/Event List window lets you define custom alarms for almost any MIB variable (OID), as long as it is present in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). You can define both rising and falling alarm thresholds for the selected MIB variables and automatically create the necessary events (to log alarm occurrences, generate a trap, or both). All aspects of alarms are user-selectable: thresholds can be established on either the absolute or delta value for a variable; events can be configured to create a log, generate a trap, or both. Using the Alarms feature, you need only be sure to select variables appropriate to the interface (Ethernet for Ethernet, Token Ring for Token Ring, etc.) when defining your alarms.

---

**NOTE:** When the RMON Alarm/Event List window is initially opened the Console Event log might show several SNMP gets/sets to the selected device. This is because Console first queries RMON status on the selected device and, if it finds that RMON is disabled, Console attempts to enable it.

---

**RMON Alarm/Event List: 10.20.33.3**

Interface: 2 - Fast Ethernet Frontpanel  
 Address: 00:00:1D:B6:9A:B7  
 Type: Ethernet CSMACD

Alarm Watch

Index	Interval	Sample	Low Threshold	Event Index	High Threshold	Event Index	Status	Alarm Var
1	00:00:05	delta	100000	2	1	1	valid	ifInOctets.2
2	00:00:05	delta	1000000	2	2	1	valid	ifInOctets.2

Event Watch

Index	Count	Last Time	Type	Description
1	3	Thu Sep 30 21:10:34 ...	log	High Threshold Exceeded-x
2	1	Thu Sep 30 21:07:44 ...	log	Low Threshold Exceeded-g
3	1004	Mon Sep 27 21:28:05 ...	log	Packet Match Occurrence
4	0	none	log	

**TIP:** You can use the RMON Alarms feature to configure alarms for MIB objects on FDDI, ATM, and other interfaces that don't specifically support RMON: the Alarm configuration lets you select any object as an alarm variable, as long as its value is defined as an integer and you assign the correct instance value.

## Alarms Watch Table

### Index

The index is a number that uniquely identifies each alarm. Index numbers are automatically assigned each time an alarm is created or modified; these numbers are random and will not necessarily be consecutive.

### Interval

Indicates the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value is compared to both the rising and falling thresholds configured for the alarm.

### Sample

Indicates whether the sample value to be compared to the thresholds is an absolute, or total value (that is, the total value counted for the selected variable), or a relative or delta value (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval.)

**LoThrshld**

Indicates the set value for the low, or falling threshold.

**Event Index**

Indicates the event index number that the falling threshold points to: this is the event that will be triggered if the falling threshold is met or crossed. If the value for this field is zero, no event will be triggered.

**HiThrshld**

Indicates the set value for the high, or rising threshold.

**Event Index**

Indicates the event index number that the rising threshold points to: the event that will be triggered if the rising threshold is met or crossed. If the value for this field is zero, no event will be triggered.

**Status**

Indicates the status of the alarm: valid, invalid, or underCreation. An alarm that is invalid is not functional and may be referring to a MIB component that is inactive (such as the Hosts component), not present, or unreachable, or it may have been deleted by software but not yet removed from memory at the device. An alarm that is underCreation is in the process of being configured (possibly by another management station), and should not be modified until its status is valid; if it never reaches valid status, it will eventually be removed.

**Alarm Variable**

Indicates the variable that is being watched. You can use the scroll bar, if necessary, to view the complete name.

*Events Watch Table***Index**

The index is a number that uniquely identifies each event. Index numbers are automatically assigned each time an event is created or modified; these numbers are random and will not necessarily be consecutive.

**LastTime**

Indicates the last time this event was triggered. Note that this information is static once it is displayed, and the LastTime field will not be updated unless you close, then open, the Alarms/Events window, or click on **Refresh**.

**Type**

Indicates the type of response that will be generated if the event is triggered: log, trap, or log & trap. A type of "none" indicates that

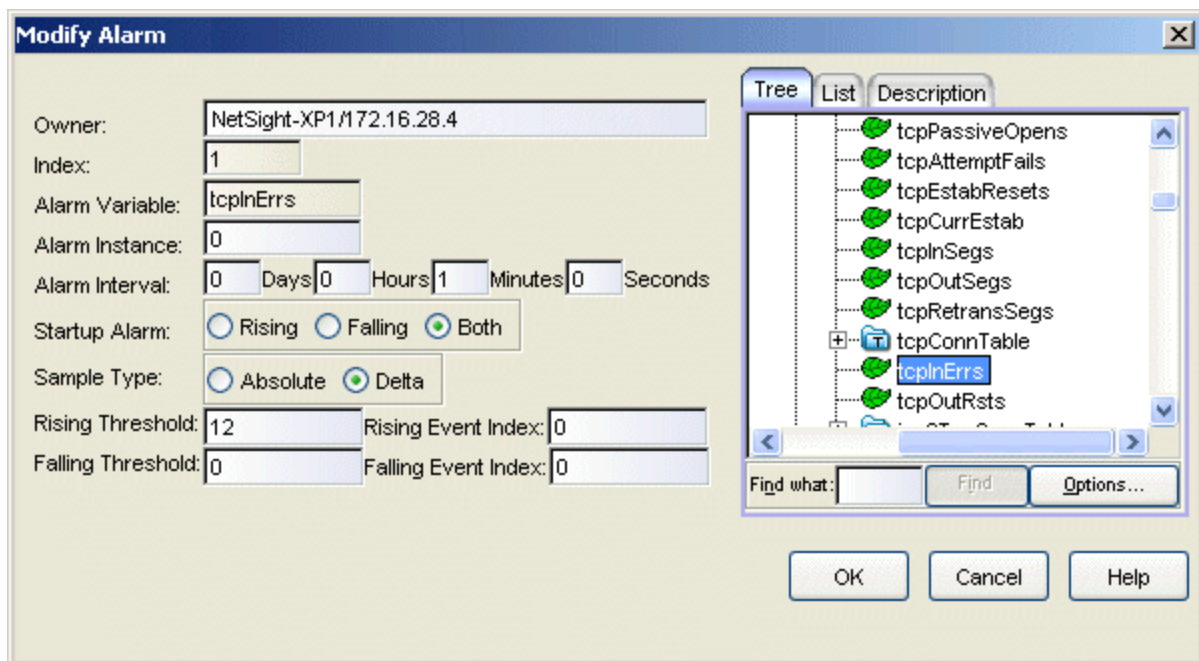
occurrences of the event will not be logged and no trap will be sent. Note that this field does not indicate, however, whether or not there are any actions associated with the selected event.

### Description

This is a user-defined text description used to identify the event and/or the alarm or packet capture that triggers it.

### Create/Modify Alarm Window

The Create Alarm and Modify Alarm windows both provide the same set of parameters to let you define alarms. The Create Alarm window is opened with default settings and allow creating new alarms. The Modify Alarm window opens showing the settings for an alarm selected in the Alarm Watch table and allows you to edit an existing alarm.



### Owner

This allows you to enter some appropriate individual as the designated owner of this alarm. This could be the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the alarm. Since any workstation can access and change the alarms you are configuring, some owner identification can prevent alarms from being altered or deleted accidentally. The default owner is the NetSight <hostname> and <IP address> <date> <time>, where

the hostname and IP address belong to the Console host system, and the date and time reflects the date and time of the alarm's creation.

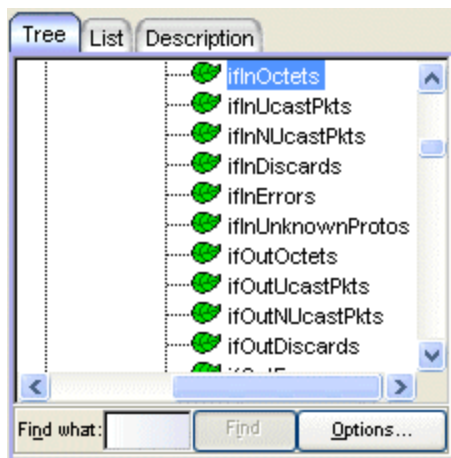
### Alarm Variable

The MIB Object Selector panel on the right side of the window contains three tabs. The **Tree** and **List** tabs let you select an **Alarm Variable** for the alarm that you are configuring. The **Description** tab shows the text description for MIB objects selected from the MIB Tree or List tab.

### Tree Tab

This tab shows the supported MIBs as a tree hierarchy. You can expand the tree to select a MIB object that you want to watch with this alarm. Once an object is selected from the tree, you can set the remaining parameters to define an instance and establish thresholds for this alarm.

#### Sample Tree Tab



### Find Feature

This feature lets you search the tree to locate a specific MIB Object by typing all or part of a text string for a particular Object ID or Description into the **Find what** field, selecting an search option, and clicking **Find**.

### List Tab

This tab presents MIB objects in a table. A table right-click menu provides find and filter features to help you locate specific MIB objects. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

Sample List Tab

Name	OID
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
ifInUnknown...	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcast...	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19

**Description Tab**

This tab displays the text description (as it appears in the MIB) for a selected MIB object.

**Alarm Instance**

RMON objects that are part of a table are instantiated by the index number that typically corresponds to an interface. For example, if you wish to set an alarm on an object located in an RMON Statistics table, you can determine the appropriate instance by noting the index number assigned to the table that is collecting data on the interface you're interested in. If there are multiple default tables per interface, however, or if additional tables have been created, this may not be true. (Table index numbers are assigned automatically as table entries are created. No two tables, even those on different interfaces, will share the same table index number.)

If you have selected an object from a table which is indexed by some other means (for example, by ring number) you must be sure to assign the instance accordingly. If you're not sure how a tabular object is instantiated, you can use the MIBTool utility to query the object; all available instances for the object will be displayed. If you have selected an object which is *not* part of a table, you must assign an instance value of 0.

If you wish to set an alarm on an object whose instance is non-integral (for example, a Host Table object indexed by MAC address) or on an object with multiple indices, like a Matrix Table entry (which is indexed by a pair of MAC addresses), you must follow certain special procedures for defining the instance. For these OIDs, the instance definition must take the following format:



table index.length(in bytes).instance(in decimal format)

For the first byte of the instance, you must use the index number of the table which contains the OID you want to track. For example, to set an alarm on an object in the Host Table, define the first byte of the instance as the index number assigned to the specific Host Table you want to check. These index numbers are assigned automatically as the table entries are created. No two tables, even if they are on different interfaces, will share the same table index number.

Second, you must specify the length, in bytes, of the index you will be using. Again, in the case of an object in the Host Table, that value would be 6, since Host Table entries are indexed by MAC address (a six-byte value).

Finally, you must specify the index itself, in decimal format. In the case of a MAC address, that means you must convert the standard hexadecimal format to decimal format. To do this, simply multiply the first digit of the two-digit hex number by 16, then add the value of the second digit. (For hex values represented by alphabetical characters, remember that a=10, b=11, c=12, d=13, e=14, and f=15.) A hex value of b7, for instance, is represented in decimal format as  $16 \times 11 + 7$ , or 183. So, for example, the instance for an object in the Hosts group might read as follows:

2.6.0.0.29.170.35.201

where 2=the host table index; 6=the length in bytes of the index to follow; and 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9.

For objects with multiple indices, such as objects in a matrix table, you must add additional length and index information to the instance definition, as illustrated below:

3.6.0.0.29.170.35.201.6.0.0.29.10.20.183

where 3=the matrix table index; 6=the length in bytes of the index to follow; 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9; 6=the length in bytes of the next index; and 0.0.29.10.20.183=the decimal format for MAC address 00-00-1d-0a-14-b7.

Additional instance issues may exist for FDDI objects. If you're unsure how to assign an instance, use the MIBTree utility to query the object of interest, and note the appropriate instancing on the returned values.

### Alarm Interval

The amount of time over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. There is no practical limit to the size of the interval (as the maximum value is 24,855 days 3 hours 14 minutes and 7 seconds -- over 68 years!). The default value is 1 minute.

### Startup Alarm

Since the first sample taken can be misleading, the Startup Alarm box lets you disable either the rising or the falling threshold for that sample only. If you want to exclude the falling alarm, select the Rising option. The first sample taken will only generate a rising alarm, even if the sample value is at or below the falling threshold. To exclude the rising alarm, select the Falling option. The first sample will then only generate a falling alarm, even if the sample value is at or above the rising threshold. If you wish to receive both alarms as appropriate, select the Both option.

### Sample Type

The Sample Type indicates whether you want your threshold values compared to the total count for the selected variable (Absolute), or to the difference between the count at the end of the current interval and the count at the end of the previous interval (Delta). Make sure you have set your thresholds accordingly.

### Rising and Falling Thresholds

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value -- either of which can indicate a network problem. To make the best use of this powerful feature, however, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom. Figure 4-8 illustrates such a configuration.

### RisingThreshold

The high threshold value for this alarm.

### RisingEventIndex

The index number of the event you would like to see triggered if the rising threshold is crossed. Assigning an invalid or zero index effectively disables the threshold, as there will be no indication that it has been crossed.

### FallingThreshold

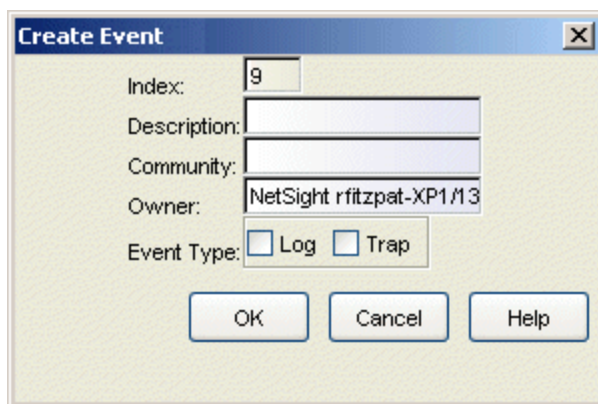
The low threshold value for this alarm.

### FallingEventIndex

The index number of the event you would like to see triggered if the falling threshold is crossed. Assigning an invalid or zero index effectively disables the threshold, as there will be no indication that it has been crossed.

## *Create/Modify Event Window*

The Create Alarm and Modify Event windows both provide the same set of parameters to let you define associate events with the alarms that you've defined and determine the specific action triggered by the event (create a log entry or trigger a trap). The Create Event window is opened with default settings and allow creating new events. The Modify Event window opens showing the settings for an event selected in the Event Watch table and allows you to edit an existing events.



### Description

Any text description that you want to identify the event. This description appears in the Events Watch window and help you distinguish among the events you have configured.

### Community

This value is included in any trap messages issued by your RMON device when this event is triggered. For EOS devices, this value is also used to direct traps related to this event to the appropriate management

workstation(s):

- If you enter a value in this field, traps related to this event will only be sent to the network management stations in the device's trap table which have been assigned the same community name (and for which traps have been enabled). Any IP addresses in the device's trap table which have not been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
- If you leave this field blank, traps related to this event will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled -- regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.

### Owner

This allows you to enter some appropriate individual as the designated owner of this event. This could be the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the event. Since any workstation can access and change the events you are configuring, some owner identification can prevent events from being altered or deleted accidentally. The default owner is the NetSight *<hostname>* and *<IP address> <date> <time>*, where the hostname and IP address belong to the Console host system, and the date and time reflects the date and time of the event's creation.

### Event Type

The Event Type determines how this event will respond when an associated threshold is crossed.

- **Log** creates log entry for the alarm associated with this event. Each event's log can be viewed by clicking on the **Event Log** button near the bottom of the [RMON Alarm/Event List](#) window.
- **Trap** instructs the device to send a pair of SNMP traps (one WARNING, one Normal) to the management station each time the event is triggered.

### *RMON Event Log*

The Event Log provides information about the alarm that triggered an event selected in the RMON Alarm/Event List window. The top portion of the window contains the device information boxes, as well as the event index number and the event description. The bottom portion lists alarm information.

Index	Time	Description
1	Mon Sep 27 15:27:27 EDT 2004	RisingAlarm: alarmIndex 1, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...
2	Thu Sep 30 15:06:24 EDT 2004	RisingAlarm: alarmIndex 2, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...
3	Thu Sep 30 15:09:14 EDT 2004	RisingAlarm: alarmIndex 2, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...

### Index

This index number is not the event's index, but a simply an index of items in the log that uniquely identifies this occurrence of the event.

### Time

Indicates the date and time of each event occurrence.

### Description

Provides a detailed description of the alarm that triggered the event: whether it was a rising or falling alarm, the alarm index number, the alarm variable name and object identifier (OID), the alarmSampleType (1=absolute value; 2=delta value), the value that triggered the alarm, the configured threshold that was crossed, and the event description. Use the scroll bar at the bottom of the log to view all the information. Each log will hold only a finite number of entries, which is determined by the resources available on the device. When the log is full, the oldest entries will be replaced by new ones.

## Related Information

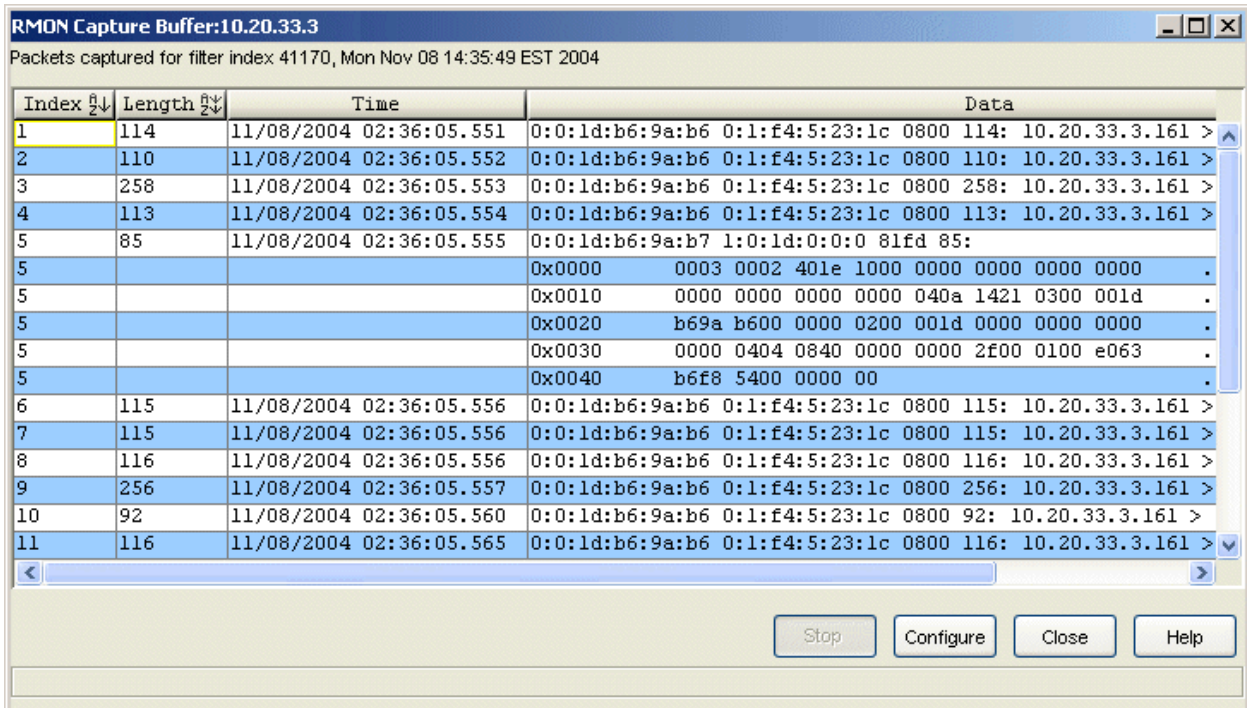
For information on related windows:

- [RMON Filter and Packet Capture Window](#)

## RMON Capture Buffer

The top portion of this window contains the filter name and index. The main portion of the window displays the captured packets.

*Sample RMON Capture Buffer Window.*



RMON Capture Buffer:10.20.33.3  
Packets captured for filter index 41170, Mon Nov 08 14:35:49 EST 2004

Index	Length	Time	Data
1	114	11/08/2004 02:36:05.551	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 114: 10.20.33.3.161 >
2	110	11/08/2004 02:36:05.552	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 110: 10.20.33.3.161 >
3	258	11/08/2004 02:36:05.553	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 258: 10.20.33.3.161 >
4	113	11/08/2004 02:36:05.554	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 113: 10.20.33.3.161 >
5	85	11/08/2004 02:36:05.555	0:0:1d:b6:9a:b7 1:0:1d:0:0:0 81fd 85: 0x0000 0003 0002 401e 1000 0000 0000 0000 0000 . 0x0010 0000 0000 0000 0000 040a 1421 0300 001d . 0x0020 b69a b600 0000 0200 001d 0000 0000 0000 . 0x0030 0000 0404 0840 0000 0000 0000 2f00 0100 e063 . 0x0040 b6f8 5400 0000 00 .
6	115	11/08/2004 02:36:05.556	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 115: 10.20.33.3.161 >
7	115	11/08/2004 02:36:05.556	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 115: 10.20.33.3.161 >
8	116	11/08/2004 02:36:05.556	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 116: 10.20.33.3.161 >
9	256	11/08/2004 02:36:05.557	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 256: 10.20.33.3.161 >
10	92	11/08/2004 02:36:05.560	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 92: 10.20.33.3.161 >
11	116	11/08/2004 02:36:05.565	0:0:1d:b6:9a:b6 0:1:f4:5:23:1c 0800 116: 10.20.33.3.161 >

Buttons: Stop, Configure, Close, Help

### Right-Click Menu

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### Configure

This button offers options that determine how the information for the Data in the captured packets is displayed in the view.

- **Default** - Displays data as a single line, showing header information and data length.
- **Short** - Displays data as a single line, showing header information, packet type, and data length.

- **Hex/ASCII** - Displays header information, type, and data as hex and ASCII.

### **Start/Stop**

These buttons control capturing when your filter is set for Continuous Capture.

---

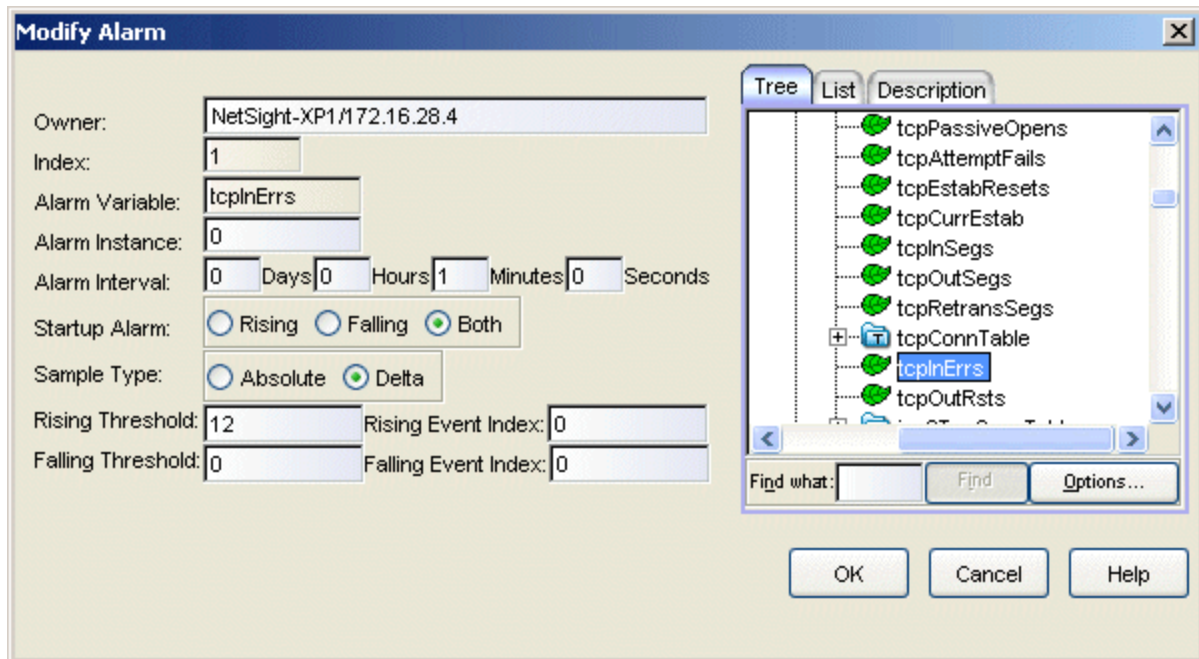
### **Related Information**

For information on related windows:

- [RMON Alarm/Event List](#)

## Create/Modify Alarm Window

The Create Alarm and Modify Alarm windows both provide the same set of parameters to let you define alarms. The Create Alarm window is opened with default settings and allow creating new alarms. The Modify Alarm window opens showing the settings for an alarm selected in the Alarm Watch table and allows you to edit an existing alarm.



### Owner

This allows you to enter some appropriate individual as the designated owner of this alarm. This could be the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the alarm. Since any workstation can access and change the alarms you are configuring, some owner identification can prevent alarms from being altered or deleted accidentally. The default owner is the NetSight *<hostname>* and *<IP address> <date> <time>*, where the hostname and IP address belong to the Console host system, and the date and time reflects the date and time of the alarm's creation.

### Alarm Variable

The MIB Object Selector panel on the right side of the window contains three tabs. The **Tree** and **List** tabs let you select an **Alarm Variable** for the

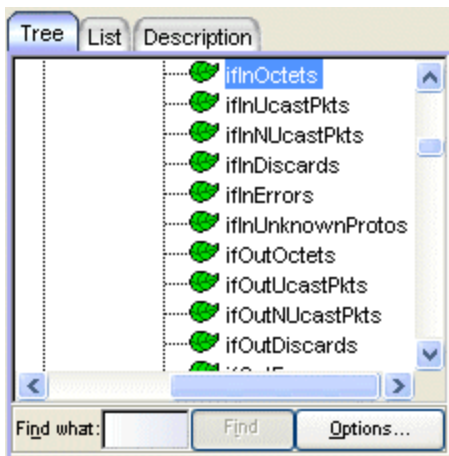


alarm that you are configuring. The **Description** tab shows the text description for MIB objects selected from the MIB Tree or List tab.

### Tree Tab

This tab shows the supported MIBs as a tree hierarchy. You can expand the tree to select a MIB object that you want to watch with this alarm. Once an object is selected from the tree, you can set the remaining parameters to define an instance and establish thresholds for this alarm.

#### Sample Tree Tab



### Find Feature

This feature lets you search the tree to locate a specific MIB Object by typing all or part of a text string for a particular Object ID or Description into the **Find what** field, selecting an search option, and clicking **Find**.

### List Tab

This tab presents MIB objects in a table. A table right-click menu provides find and filter features to help you locate specific MIB objects. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

Sample List Tab

The screenshot shows a window with three tabs: 'Tree', 'List', and 'Description'. The 'List' tab is active, displaying a table with two columns: 'Name' and 'OID'. The table contains the following data:

Name	OID
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
ifInUnknown...	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcast...	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19

**Description Tab**

This tab displays the text description (as it appears in the MIB) for a selected MIB object.

**Alarm Instance**

RMON objects that are part of a table are instanced by the index number that typically corresponds to an interface. For example, if you wish to set an alarm on an object located in an RMON Statistics table, you can determine the appropriate instance by noting the index number assigned to the table that is collecting data on the interface you're interested in. If there are multiple default tables per interface, however, or if additional tables have been created, this may not be true. (Table index numbers are assigned automatically as table entries are created. No two tables — even those on different interfaces — will share the same table index number.)

If you have selected an object from a table which is indexed by some other means — for example, by ring number — you must be sure to assign the instance accordingly. If you're not sure how a tabular object is instanced, you can use the MIBTool utility to query the object; all available instances for the object will be displayed. If you have selected an object which is *not* part of a table, you must assign an instance value of 0.

---

**NOTE:** If you wish to set an alarm on an object whose instance is non-integral — for example, a Host Table object indexed by MAC address — or on an object with multiple indices, like a Matrix Table entry (which is indexed by a pair of MAC addresses), you must follow certain special procedures for defining the instance. For these OIDs, the instance definition must take the following format:

table index.length(in bytes).instance(in decimal format)

For the first byte of the instance, you must use the index number of the table which contains the OID you want to track. For example, to set an alarm on an object in the Host Table, define the first byte of the instance as the index number assigned to the specific Host Table you want to check. These index numbers are assigned automatically as the table entries are created. No two tables — even if they are on different interfaces — will share the same table index number.

Second, you must specify the length, in bytes, of the index you will be using. Again, in the case of an object in the Host Table, that value would be 6, since Host Table entries are indexed by MAC address — a six-byte value.

Finally, you must specify the index itself, in decimal format. In the case of a MAC address, that means you must convert the standard hexadecimal format to decimal format. To do this, simply multiply the first digit of the two-digit hex number by 16, then add the value of the second digit. (For hex values represented by alphabetical characters, remember that a=10, b=11, c=12, d=13, e=14, and f=15.) A hex value of b7, for instance, is represented in decimal format as  $16 \times 11 + 7$ , or 183. So, for example, the instance for an object in the Hosts group might read as follows:

2.6.0.0.29.170.35.201

where 2=the host table index; 6=the length in bytes of the index to follow; and 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9.

For objects with multiple indices — such as objects in a matrix table — you must add additional length and index information to the instance definition, as illustrated below:

3.6.0.0.29.170.35.201.6.0.0.29.10.20.183

where 3=the matrix table index; 6=the length in bytes of the index to follow; 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9; 6=the length in bytes of the next index; and 0.0.29.10.20.183=the decimal format for MAC address 00-00-1d-0a-14-b7.

Additional instance issues may exist for FDDI objects. If you're unsure how to assign an instance, use the MIBTree utility to query the object of interest, and note the appropriate instancing on the returned values.

---

### Alarm Interval

The amount of time over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. There is no practical limit to the size of the interval (as the maximum value is 24,855 days 3 hours 14 minutes and 7 seconds — over 68 years!). The default value is 1 minute.

### Startup Alarm

Since the first sample taken can be misleading, the Startup Alarm box lets you disable either the rising or the falling threshold for that sample only. If you want to exclude the falling alarm, select the Rising option. The first sample taken will only generate a rising alarm, even if the sample value is at or below the falling threshold. To exclude the rising alarm, select the Falling option. The first sample will then only generate a falling alarm, even if the sample value is at or above the rising threshold. If you wish to receive both alarms as appropriate, select the Both option.

### Sample Type

The Sample Type indicates whether you want your threshold values compared to the total count for the selected variable (Absolute), or to the difference between the count at the end of the current interval and the count at the end of the previous interval (Delta). Make sure you have set your thresholds accordingly.

### Rising and Falling Thresholds

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value — either of which can indicate a network problem. To make the best use of this powerful feature, however, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom. Figure 4-8 illustrates such a configuration.

### Rising Threshold

The high threshold value for this alarm.

**RisingEventIndex**

The index number of the event you would like to see triggered if the rising threshold is crossed. Assigning an invalid or zero index effectively disables the threshold, as there will be no indication that it has been crossed.

**FallingThreshold**

The low threshold value for this alarm.

**FallingEventIndex**

The index number of the event you would like to see triggered if the falling threshold is crossed. Assigning an invalid or zero index effectively disables the threshold, as there will be no indication that it has been crossed.

---

**Related Information**

For information on related windows:

- [RMON Packet Capture Window](#)
- [Create/Modify Event Window](#)
- [RMON Alarm/Event List](#)

## RMON Create/Modify Filter Window

The Create and Modify Filter windows let you add a new RMON filter or modify an existing filter. When you create a filter, you define the criteria that must be met in order for a packet to be captured. All filter elements selected via the Create Filter window are linked by logical ANDs, meaning a packet must meet all selected criteria before it will be considered a match.

**Create Filter**

Filter Index: 0                      Interface: 2

Description: Fri Sep 24 15:29:25 EDT 2004

Owner: NetSight-XP1/172.16.28.4

**Address Parameters**

Address

IP     MAC

Dest     Source

Bilateral

Pair

D: \_\_\_\_\_

S: \_\_\_\_\_

**Buffer Parameters**

Available Device Memory: 1033K

Capture Buffer: 50 K

Number of Packets: \_\_\_\_\_

Continuous Capture

**Capture**

Whole Packet

1st 128 Bytes

**Patterns**

Pattern Match

- LLC 0x0f0 NetBIOS
- Novell DIX 0x8138
- LLC SNA 0x04
- 802.3 Raw
- LLC 0xe0 IPX
- DEC LAT 0x6004
- DECnet phase IV (Token Ring)
- Novell IPX DIX (Token Ring)

**Filter Parameters**

Capture:  On     Off

Capture Type:  Match     Fail

**Status Parameters**

Status

Good

OK    Cancel    Help

**NOTE:** The index numbers are random, and will not necessarily be sequential.

### Description

This is a text description that you can enter to identify the filter. This description will appear in the Filter List and help you distinguish among the filters you have configured. Note that the description defaults to the current date and time. This default (timestamp) is also used if you leave the description field blank.

### Owner

This allows you to enter some appropriate individual as the designated owner of this filter. This could be the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the filter. Since any workstation can access and change the filters you are configuring, some owner identification can prevent filters from being altered or deleted accidentally. The default owner is the NetSight *<hostname>* and *<IP address> <date> <time>*, where the hostname and IP address belong to the Console host system, and the date and time reflects the date and time of the filter's creation.

### Address Parameters

Address Parameters let you filter packets based on one or more addresses. The filter can be defined to specify packets according to combinations of: Address Type, and Source and Destination addresses. The remaining Address Parameters are activated once an address type (IP or MAC) has been selected.

### Destination

Lets you filter packets based on a specific destination MAC or IP address and fill in the desired address in the **D:**field.

### Source

Lets you filter packets based on a specific source MAC or IP address and fill in the desired address in the **S:** field.

### Bilateral

Selecting **Bilateral** filters all packets going to or coming from a single specific IP Address or MAC address as specified in the **B:** field.

### Pair

**Pair** lets you filter all packets travelling in both directions between two specific stations. Enter the appropriate IP Addresses or MAC addresses in the **1:** and **2:** fields.

**NOTE:** It doesn't matter which address is entered in which field, as the filter will be applied to all traffic between the two.

---

### Patterns

When Pattern Match is checked, you can filter packets based on one or more protocol type(s) selected from associated list.

---

**NOTE:** The list of patterns displayed will vary depending on type of device/interface where the filter is being applied.

---

### Buffer Parameters

This section lets you control the amount of device memory that will be allocated to the filter's capture buffer, and determine how that memory will be used:

- The **Available Device Memory** field displays the total amount of device memory currently available for use as a capture buffer. You can enter the amount of memory (in kilobytes) that you wish to reserve for this filter's capture buffer in the **Capture Buffer Size** field. The value in this field will default to 50K or the total available memory, whichever is less.
- **Continuous Capture** lets you set the filter's buffer to be circular -- that is, once the buffer is full, the oldest entries will be replaced by the newest ones. If this option is not selected, the buffer will stop capturing packets once it is full. Note that if you select **Continuous Capture**, the **Whole Packets** option will be grayed out, and the value in the **1st\_\_Bytes** field will automatically be fixed at 128K.
- **Whole Packet**, when selected, lets you store each matched packet in its entirety.
- **1st\_ Bytes** lets you enter the number of bytes to capture when only you want to capture a portion of each matched packet. This option is only active if the **Whole Packets** option is *not* selected.
- **Number of Packets** - This button will show the approximate number of packets that will be captured with the current buffer settings. If too many or too few packets will be captured, you can adjust your parameters accordingly. Note that the number provided is approximate, and under certain conditions more or fewer packets may be captured.



### Filter Parameters

The **Filter Parameters** section lets you define the actions that will be associated with your filter:

#### Capture:

- **On** - enable the filter
- **Off** - disable the filter (All packets will still be matched against disabled filters (as indicated by the Packets Matched field in the main Packet Capture window), but none will be captured to that filter's buffer.)

#### Capture Type:

- **Match** - capture packets that match filter parameters
- **Fail** - capture packets that do *not* match the filter.

### Status

If you are creating/modifying a filter for Ethernet packets, you can capture packets based on packet status by selecting **Status**. Once selected, the associated menu is activated, offering choices of Ethernet packet status (Good, Bad, Fragments, Jabbers, Runts, Giants, and CRC/Align). The Status feature is not available for Token Ring devices.

---

**NOTE:** You can select one, two, or all three filter components for any one filter; however, keep in mind that these filter criteria are linked by logical ANDs, and the more specific the filter, the fewer the packets that will be matched.

---

### Related Information

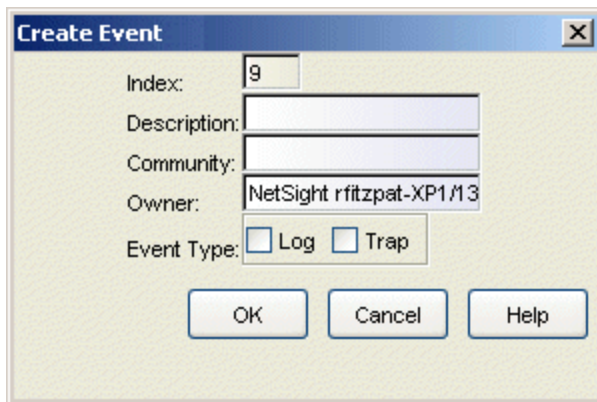
For information on related windows:

- [RMON Alarm/Event List](#)
- [Create/Edit Alarm Window](#)
- [Create/Edit Event Window](#)
- [RMON Packet Capture](#)

## Create/Modify Event Window

---

The Create Alarm and Modify Event windows both provide the same set of parameters to let you associate events with the alarms that you've defined and determine the specific action triggered by the event (create a log entry or trigger a trap). The Create Event window is opened with default settings and allows you to create a new event. The Modify Event window opens showing the settings for an event selected in the Event Watch table and allows you to edit that event.



### Description

Any text description that you want to identify the event. This description appears in the Events Watch window and helps you distinguish among the events you have configured.

### Community

This value is included in any trap messages issued by your RMON device when this event is triggered. For EOS devices, this value is also used to direct traps related to this event to the appropriate management workstation(s):

- If you enter a value in this field, traps related to this event will only be sent to the network management stations in the device's trap table that have been assigned the same community name (and for which traps have been enabled). Any IP addresses in the device's trap table that have not been assigned the same community string, or that have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
- If you leave this field blank, traps related to this event will be sent to any network management stations that have been added to the device's trap table, and for which traps have been enabled —

regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.

### Owner

This allows you to enter some appropriate individual as the designated owner of this event. This could be the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the event. Since any workstation can access and change the events you are configuring, some owner identification can prevent events from being altered or deleted accidentally. The default owner is the NetSight *<hostname>* and *<IP address> <date> <time>*, where the hostname and IP address belong to the Console host system, and the date and time reflects the date and time of the event's creation.

### Event Type

The Event Type determines how this event will respond when an associated threshold is crossed.

- **Log** creates log entry for the alarm associated with this event. Each event's log can be viewed by clicking on the **Event Log** button near the bottom of the [RMON Alarm/Event List](#) window.
- **Trap** instructs the device to send a pair of SNMP traps (one WARNING, one Normal) to the management station each time the event is triggered.

### *RMON Event Log*

The Event Log provides information about the alarm that triggered an event selected in the [RMON Alarm/Event List](#) window. The top portion of the window contains the device information boxes, as well as the event index number and the event description. The bottom portion lists alarm information.

Index	Time	Description
1	Mon Sep 27 15:27:27 EDT 2004	RisingAlarm: alarmIndex 1, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...
2	Thu Sep 30 15:06:24 EDT 2004	RisingAlarm: alarmIndex 2, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...
3	Thu Sep 30 15:09:14 EDT 2004	RisingAlarm: alarmIndex 2, alarmVariable 1.3.6.1.2.1.2.2.1.10.2, alarmSampleT...

### Index

This index number is not the event's index, but a simply an index of items in the log that uniquely identifies this occurrence of the event.

### Time

Indicates the date and time of each event occurrence.

### Description

Provides a detailed description of the alarm that triggered the event: whether it was a rising or falling alarm, the alarm index number, the alarm variable name and object identifier (OID), the alarmSampleType (1=absolute value; 2=delta value), the value that triggered the alarm, the configured threshold that was crossed, and the event description. Use the scroll bar at the bottom of the log to view all the information. Each log will hold only a finite number of entries, which is determined by the resources available on the device. When the log is full, the oldest entries will be replaced by new ones.

---

## Related Information

For information on related windows:

- [RMON Filter and Packet Capture Window](#)
- [Create/Modify Alarm Window](#)
- [RMON Alarm/Event List](#)

## RMON Ethernet Statistics Window

---

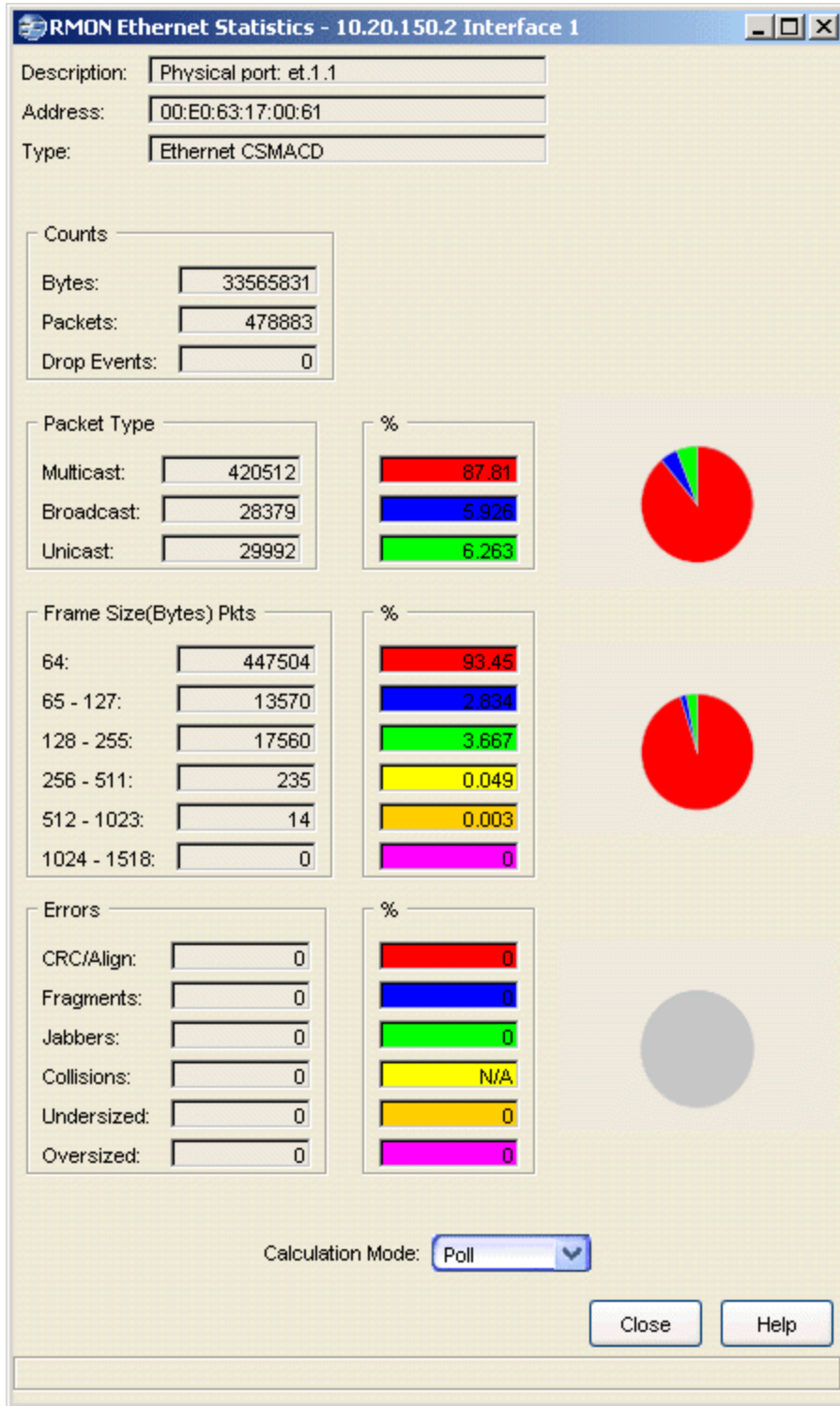
Use this window to view a detailed statistical breakdown of traffic on the monitored Ethernet network segment. When viewing this window, keep in mind that the data provided applies only to the interface or network segment. If you reset your device, close and re-open this window to refresh the values.

---

**NOTE:** When the RMON Ethernet Statistics window is initially opened the Console Event log might show several SNMP gets/sets to the selected device. This is because Console first queries RMON status on the selected device and, if it finds that RMON is disabled, Console attempts to enable it.

---

To access the RMON Ethernet Statistics window from Device Manager, click on the desired port in the Device View and select RMON Ethernet Statistics from the port menu. To access this window from Console, select the desired port in the Port View of the Properties tab or in a FlexView table, and use the right-click menu option.



**Description**

Displays a description of the port and the type of interface followed by the board and port number.

**Address**

Displays the physical address of the selected port.

**Type**

Displays the type of interface.

**Counts**

Displays the total number of bytes and packets processed on the network segment and the total number of packets dropped.

- **Bytes** -- Displays the total number of bytes contained in packets processed on the network segment. This number includes bytes contained in error packets.
- **Packets** -- Displays the total number of packets processed on the network segment. This number includes error packets.
- **Drop Events** -- Displays the number of times packets were dropped because the device could not keep up with the flow of traffic on the network. (This value reflects the number of times packets were dropped not the actual number of packets.)

**Packet Type**

Displays the total number and percentage of good packets transmitted on the network segment that were Multicast, Broadcast, and Unicast. The pie chart presents a graphical view of the percentage breakdown and the colors in the pie chart correspond to the colors in the percentage display boxes.

- **Multicast** -- Displays the number of good packets processed on the network segment that were destined for more than one address. This total does not include broadcast packets. The number under the percentage column indicates what percentage of good packets transmitted on the network segment were multicast.
- **Broadcast** -- Displays the number of good packets processed on the network segment that had the broadcast (FF-FF-FF-FF-FF-FF) destination address. The number under the percentage column indicates what percentage of good packets transmitted on the network segment were broadcast.
- **Unicast** -- Displays the number of good packets processed on the network segment that were destined for a single address. The number under the percentage column indicates what percentage of good packets transmitted on the network segment were unicast.

### Frame Size (Bytes) Pkts

Displays the number of packets (including error packets) within these lengths (excluding framing bits but including frame check sequence bits) processed by the network segment. The pie chart presents a graphical view of the percentage breakdown and the colors in the pie chart correspond to the colors in the percentage display boxes.

### Errors

Displays the type and number of problem packets processed by the network segment. The pie chart presents a graphical view of the percentage breakdown and the colors in the pie chart correspond to the colors in the percentage display boxes.

- **CRC/Align** -- Displays the number of packets processed by the network segment that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclical Redundancy Check (CRC) error).
- **Fragments** -- Displays the number of packets processed by the network segment that were undersized (less than 64 bytes in length (runt)) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
- **Jabbers** -- Displays the number of packets processed by the network segment that were oversized (greater than 1518 bytes (giant)) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
- **Collisions** -- Displays the total number of receive (those the device detects while receiving a transmission) and transmit (those the device detects while transmitting) collisions detected on the network segment. The percentage field for Collisions will always display N/A because collisions are not true errors; percentages are not calculated, and will not be represented in the pie chart.
- **Undersized** -- Displays the number of packets processed by the network segment that contained fewer than 64 bytes (runt packets), but were otherwise well-formed.
- **Oversized** -- Displays the number of packets processed by the network segment that contained more than 1518 bytes (giant packets), but were otherwise well-formed.

### Calculation Mode

Use the drop-down list to specify how the statistics count will be calculated:



- **Poll** -- After the completion of the current polling cycle plus one complete polling cycle, the window will display the total count of statistics processed since the device was last initialized. These totals are updated after each polling cycle.
  - **Delta** -- After the completion of the current polling cycle plus two more polling cycles, the window will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.
  - **Accumulate** -- After the completion of the current polling cycle plus two more polling cycles, the window will display a fresh cumulative count of statistics. This option does not clear the device counters; you can still re-select Poll for the total count since the device was last initialized.
- 

### Related Information

For information on related windows:

- [Interface Statistics Window](#)

## RMON History Window

---

The RMON History window displays an individual history table selected from the [RMON History List window](#). History tables collect snapshots of network statistics taken at user-defined intervals, and present them in either numerical or graphical format. Use the tables to look at historical views of performance, thereby gaining a better sense of how network performance changes from sample interval to sample interval. Statistics collection begins when the device is initialized or reset. As new entries are added, the window is automatically updated.

---

**NOTE:** When the RMON History window is initially opened the Console Event log might show several SNMP gets/sets to the selected device. This is because Console first queries RMON status on the selected device and, if it finds that RMON is disabled, Console attempts to enable it.

---

To access this window, select the desired history table entry in the RMON History List window, and click **View**. The RMON History window opens.

RMON history statistics can be viewed in numerical (Table view) or graphical (Graph view) format by selecting the appropriate tab:

- [Table View](#)
- [Graph View](#)

### *Table View*

Selecting the **Table View** tab displays the history statistics in a numerical format. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**RMON History: 12.22.23.48**

Interface: 23 - Gigabit Ethernet Frontpanel port 23  
 Address: 00:01:F4:6C:A8:42  
 Type: Ethernet CSMA/CD  
 History Index: 15

Table View | Graph View

Index	% Load	Date	Time	Packets	Bcast Pkts	Mcast Pkts	Ucast Pkts	Octets
351	0.0	07/28/2005	09:43:54	359	64	147	148	47162
352	0.0	07/28/2005	09:46:24	308	50	148	110	40214
353	0.0	07/28/2005	09:48:54	855	86	147	622	107238
354	0.0	07/28/2005	09:51:24	344	64	149	131	43444
355	0.0	07/28/2005	09:53:54	348	62	146	140	46061
356	0.0	07/28/2005	09:56:24	326	58	148	120	41874
357	0.0	07/28/2005	09:58:54	321	47	146	128	43355
358	0.0	07/28/2005	10:01:24	308	51	151	106	39899
359	0.0	07/28/2005	10:03:54	793	55	148	590	101309
360	0.0	07/28/2005	10:06:24	386	64	148	174	49463

Import Export Print Close Help

Records received: 24

## Interface

Displays a brief description of the interface.

## Address

Displays the MAC address for the selected interface.

## Type

Displays the interface type.

## History Index

Displays a number that uniquely identifies the selected history table.

## Table Area

Displays a list of network statistics collected at user-defined intervals in a numerical format.

## Index

Displays a number that uniquely identifies each history table entry. The first entry -- collected at the appropriate interval after the device was initialized -- is indexed with a 1. Regardless of the maximum number of entries defined for the table, the sample index continues to increment until the device is reset.

**% Load**

Displays the interface load during the sample interval, in hundredths of a percent.

**Date**

Displays the date the sample was taken.

**Time**

Displays the time the sample was taken. This time reflects the beginning of the sampling interval (e.g., a time value of 8:59:13 on the 30 second table indicates that the statistical data was collected from 8:59:13 to 8:59:42).

**Packets**

Displays the total number of packets received during the sample interval. This number includes error packets.

**Bcast Pkts**

Displays the number of good packets received during the sample interval that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.

**Mcast Pkts**

Displays the number of good packets received during the sample interval that were directed to a multicast address. This total does not include broadcast packets.

**Ucast Pkts**

Displays the number of good packets received during the sample interval that were directed to a single address.

**Octets**

Displays the total number of octets, or bytes, received during the sample interval. This number includes octets contained in error packets.

**Drop Events**

Displays the number of times during the sample interval that packets were dropped because the device could not keep up with the flow of traffic on the network segment. This value reflects the number of times packets were dropped.

**CRC Align**

Displays the number of packets received during the sample interval that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check (CRC) error).

**Undersize**

Displays the number of packets received during the sample interval that contained fewer than 64 bytes (runt packets), but were otherwise well-formed.

**Oversize**

Displays the number of packets received during the sample interval that contained more than 1518 bytes (giant packets), but were otherwise well-formed.

**Fragments**

Displays the number of packets received during the sample interval that were undersized (less than 64 bytes in length; a runt packet) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

**Jabbers**

Displays the number of packets received during the sample interval that were oversized (greater than 1518 bytes; a giant packet) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

**Collisions**

Displays the total number of receive (detected while the device was receiving a transmission) and transmit (detected while the device was transmitting) collisions detected on the network segment during the sample interval.

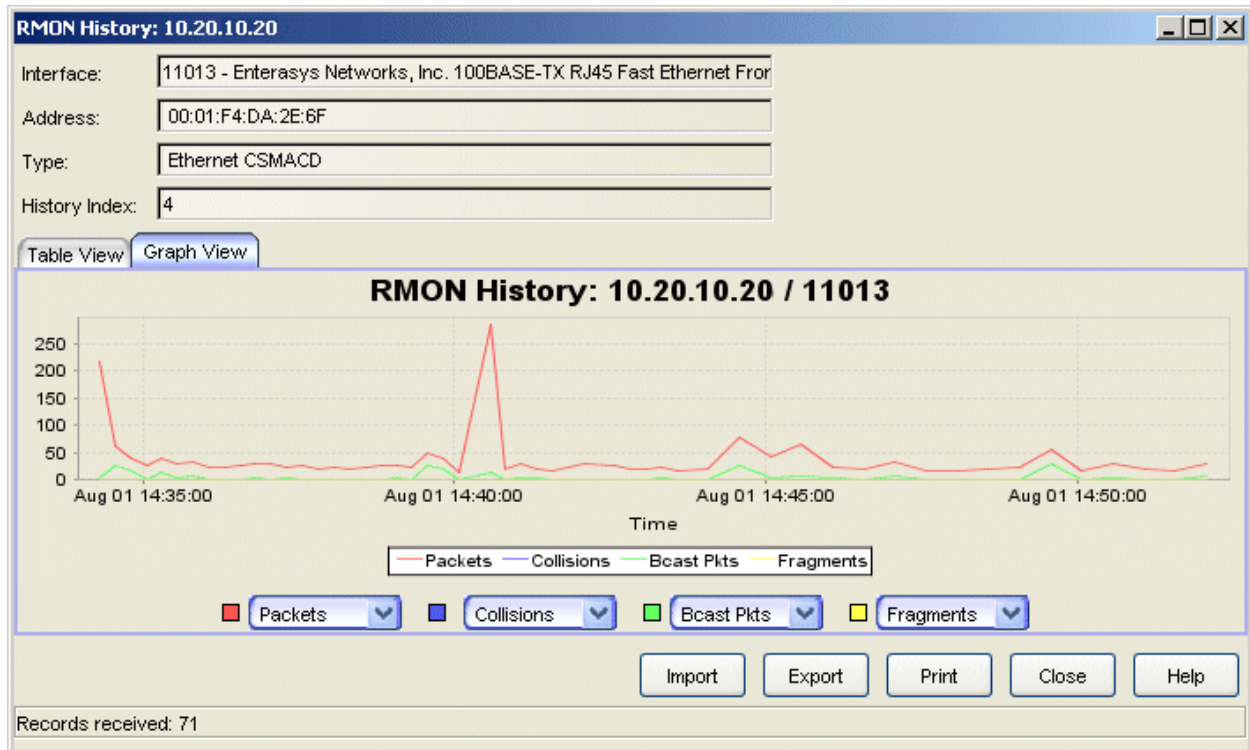
*Graph View*

Selecting the **Graph View** tab displays the history statistics in a graph format. As many as four variables can be displayed in the graph at once. Use the drop-down lists to select the desired variables.

---

**NOTE:** The selected variable with the largest value controls the scale, making it difficult to graph variables with large values at the same time as variables with small values. If you have difficulty displaying error-type variables, which typically have low values, use the Nothing selection as one or more of your variables.

---



### Interface

Displays a brief description of the interface.

### Address

Displays the MAC address for the selected interface.

### Type

Displays the interface type.

### History Index

Displays a number that uniquely identifies the selected history table.

### Graph Area

Displays a graph of network statistics collected at user-defined intervals.

### Number of Units

Displays the number of units counted for each of the selected variables during the sample interval.

### Time

Displays the date and time the sample was taken. The time reflects the beginning of the sampling interval (e.g., a time value of 8:59:13 on the 30 second table indicates that the statistical data was collected from 8:59:13 to 8:59:42).

## Drop-down Lists

Use the four drop-down lists to select the variables to be displayed in the graph: [Drop Events](#), [Octets](#), [Packets](#), [Bcast Pkts](#), [Mcast Pkts](#), [Ucast Pkts](#), [CRC Align](#), [Oversize](#), [Undersize](#), [Fragments](#), [Jabbers](#), [Collisions](#), [% Load](#), or Nothing.

---

**NOTE:** The selected variable with the largest value controls the scale, making it difficult to graph variables with large values at the same time as variables with small values. If you have difficulty displaying error-type variables, which typically have low values, use the Nothing selection as one or more of your variables.

---

To the left of the drop-down list is the variable's corresponding line color.

## Import Button

Opens the Import From window where you can import table data previously exported to a \*.csv file. This allows you to view previous history table statistics.

## Export Button

Opens the Save As window where you can export table data in comma separated variable (\*.csv) format. The data can then be imported into any database or spreadsheet software that accepts comma-delimited data.

## Print Button

Prints the contents of the RMON History window.

---

## Related Information

For information on related tasks:

- [RMON History List Window](#)
- [Create/Modify History Window](#)

## RMON History List Window

---

Use this window to view a list of RMON history tables for a selected port (interface). History tables collect snapshots of network statistics taken at user-defined intervals. On Extreme and Enterasys devices, each interface has two default history tables. One table contains snapshots taken every 30 minutes, and the other contains snapshots taken every 30 seconds. You can use the [RMON History](#) window to view each table of statistics in numerical or graphical format.

---

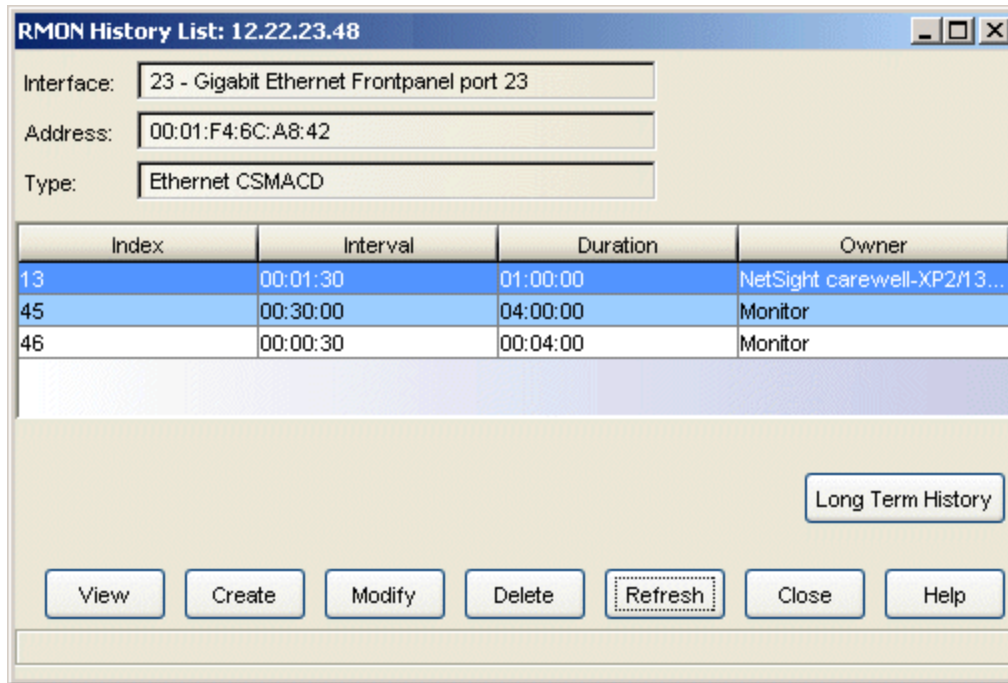
**NOTE:** When the RMON History List window is initially opened, the Console Event log might show several SNMP gets/sets to the selected device. This is because Console first queries RMON status on the selected device and, if it finds that RMON is disabled, Console attempts to enable it.

---

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the RMON History List window from Device Manager, click on the desired port in the Device View and select RMON History List from the port menu. To access this window from Console, select the desired port in the Port View of the Properties tab or in a FlexView table, and use the right-click Port Tools menu option.





### Interface

Displays a brief description of the selected interface.

### Address

Displays the MAC address for the selected interface.

### Type

Displays the interface type.

### Index

Displays a number that uniquely identifies each history table.

### Interval

Displays the time interval applicable to each table sample. For the default tables, statistical data is collected either every 30 seconds or every 30 minutes.

### Duration

Displays the maximum range of time covered by each table. This maximum range defines the number of table entries. For example, the durations assigned to the default tables ensure that each table will hold a maximum of 120 entries. Therefore, the oldest sample in the 30-second table will be one hour old, and the oldest sample in the 30-minute table will be 2 1/2 days old. Once the tables are full, the oldest sample is replaced with the newest.

**Owner**

Displays the owner, or originator, of the request to create the history table. Any request initiated by the RMON agent (i.e., the default host tables) shows its owner as monitor. For user-created tables, this field displays the owner text string entered during the create history process.

**Long Term History Button**

Opens the [RMON Long Term History List](#) window where you can view all the history tables that have been configured for long term monitoring.

**View Button**

Opens the [RMON History](#) window where you can view the selected history table.

**Create Button**

Opens the [Create History](#) window where you can create a new RMON history table.

**Modify Button**

Opens the [Modify History](#) window where you can modify the parameters of the selected RMON history table.

**Delete Button**

Select a history table, and click **Delete** to remove the table from the list. When any history table is deleted, the index numbers of the remaining tables remain the same and the list is no longer sequential. If you deleted table index 3, the table list would read 1, 2, 4, 5,...etc. Missing index numbers are automatically re-used when new tables are created.

**CAUTION:** It is recommended that you do not delete a table of which you are not the owner. To restore deleted default tables, either recreate them or reset the device to restore all firmware defaults. Resetting the device, however, deletes any new tables that have been created.

---

**Refresh Button**

Displays updated history list information. The history list is automatically refreshed each time you create, modify, or delete an entry.

---

**Related Information**

For information on related windows:

- [RMON History Window](#)
- [Create/Modify History Window](#)

## RMON Long Term History Window

---

The RMON Long Term History window displays an individual long term history file selected from the [RMON Long Term History List](#) window.

The long term history function automatically saves data from a device's history table to a comma separated variable file (\*.csv) on the client workstation. The data can then be viewed in this window, or imported into any database or spreadsheet software that accepts comma-delimited data. With Long Term History, it is not necessary to manually export data (via the Export button in the RMON History window).

---

**NOTE:** The [RMON History List](#) window must remain open for the history data to be saved to the .csv file.

---

To access this window, select the desired history table file in the RMON Long Term History List window, and click **View**.

RMON history statistics can be viewed in numerical (Table view) or graphical (Graph view) format by selecting the appropriate tab:

- [Table View](#)
- [Graph View](#)

### *Table View*

Selecting the **Table View** tab displays the long term history statistics in a numerical format. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

Interface: 3 - Fast Ethernet Frontpanel  
 Address: 00:00:1D:D4:D8:0C  
 Type: Ethernet CSMACD  
 History Index: 35

Table View Graph View

Index	% Load	Date	Time	Packets	Bcast Pkts	Mcast Pkts	Ucast Pkts	Octets
1	0.0	07/27/2005	14:39:08	69	31	22	16	6764
2	0.0	07/27/2005	14:39:38	43	2	23	18	4650
3	0.0	07/27/2005	14:40:08	54	1	23	30	6619
4	0.0	07/27/2005	14:40:38	45	5	22	18	4111
4	0.0	07/27/2005	14:40:38	45	5	22	18	4111
5	0.0	07/27/2005	14:41:08	39	3	24	12	3948
6	0.0	07/27/2005	14:41:38	40	9	23	8	3542
7	0.0	07/27/2005	14:42:08	49	3	22	24	5935
8	0.0	07/27/2005	14:42:38	41	2	23	16	4395
9	0.0	07/27/2005	14:43:08	48	0	24	24	5877

Print Close Help

Records received: 43

### Interface

Displays a brief description of the selected interface.

### Address

Displays the MAC address for the selected interface.

### Type

Displays the interface type.

### History Index

Displays a number that uniquely identifies the selected history table.

### Table Area

Displays a list of network statistics collected at user-defined intervals in a numerical format.

### Index

Displays a number that uniquely identifies each history table entry. The first entry -- collected at the appropriate interval after the device was initialized -- is indexed with a 1. Regardless of the maximum number of entries defined for the table, the index continues to increment until the device is reset. However, if a history table is modified so that the interval and/or duration change, the long-term history of that table will continue to store all

data, but the Index column will reset to 1 with the first snapshot under the new parameters.

**% Load**

Displays the interface load during the sample interval, in hundredths of a percent.

**Date**

Displays the date the sample was taken.

**Time**

Displays the time the sample was taken. This time reflects the beginning of the sampling interval (e.g., a time value of 8:59:13 on the 30 second table indicates that the statistical data was collected from 8:59:13 to 8:59:42).

**Packets**

Displays the total number of packets received during the sample interval. This number includes error packets.

**Bcast Pkts**

Displays the number of good packets received during the sample interval that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.

**Mcast Pkts**

Displays the number of good packets received during the sample interval that were directed to a multicast address. This total does not include broadcast packets.

**Ucast Pkts**

Displays the number of good packets received during the sample interval that were directed to a single address.

**Octets**

Displays the total number of octets, or bytes, received during the sample interval. This number includes octets contained in error packets.

**Drop Events**

Displays the number of times during the sample interval that packets were dropped because the device could not keep up with the flow of traffic on the network segment. This value reflects the number of times packets were dropped.

**CRC Align**

Displays the number of packets received during the sample interval that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check (CRC) error).

**Undersize**

Displays the number of packets received during the sample interval that contained fewer than 64 bytes (runt packets), but were otherwise well-formed.

**Oversize**

Displays the number of packets received during the sample interval that contained more than 1518 bytes (giant packets), but were otherwise well-formed.

**Fragments**

Displays the number of packets received during the sample interval that were undersized (less than 64 bytes in length; a runt packet) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

**Jabbers**

Displays the number of packets received during the sample interval that were oversized (greater than 1518 bytes; a giant packet) and had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).

**Collisions**

Displays the total number of receive (detected while the device was receiving a transmission) and transmit (detected while the device was transmitting) collisions detected on the network segment during the sample interval.

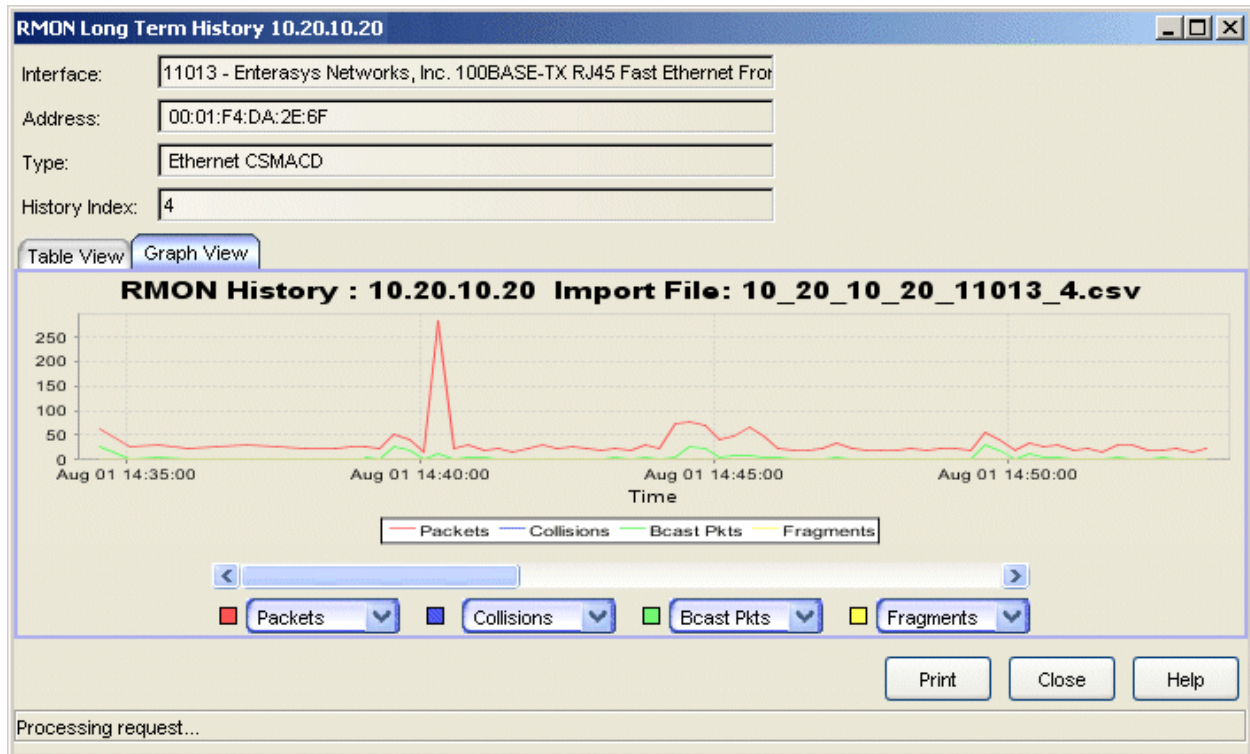
*Graph View*

Selecting the **Graph View** tab displays the history statistics in a graph format. As many as four variables can be displayed in the graph at once. Use the drop-down lists to select the desired variables.

---

**NOTE:** The selected variable with the largest value controls the scale, making it difficult to graph variables with large values at the same time as variables with small values. If you have difficulty displaying error-type variables, which typically have low values, use the Nothing selection as one or more of your variables.

---



### Interface

Displays a brief description of the interface.

### Address

Displays the MAC address for the selected interface.

### Type

Displays the interface type.

### History Index

Displays a number that uniquely identifies the selected history table.

### Graph Area

Displays a graph of network statistics collected at user-defined intervals.

### Number of Units

Displays the number of units counted for each of the selected variables during the specified interval.

### Time

Displays the date and time the sample was taken. The time reflects the beginning of the sampling interval (e.g., a time value of 8:59:13 on the 30

second table indicates that the statistical data was collected from 8:59:13 to 8:59:42).

### Drop-down Lists

Use the four drop-down lists to select the variables to be displayed in the graph: [Drop Events](#), [Octets](#), [Packets](#), [Bcast Pkts](#), [Mcast Pkts](#), [Ucast Pkts](#), [CRC Align](#), [Oversize](#), [Undersize](#), [Fragments](#), [Jabbers](#), [Collisions](#), [% Load](#), or Nothing. To the left of the drop-down list is the variable's corresponding line color.

---

**NOTE:** The selected variable with the largest value controls the scale, making it difficult to graph variables with large values at the same time as variables with small values. If you have difficulty displaying error-type variables, which typically have low values, use the Nothing selection as one or more of your variables.

---

### Print Button

Prints the contents of the RMON Long Term History window.

---

### Related Information

For information on related tasks:

- [RMON Long Term History List Window](#)
- [Create/Modify History Window](#)



## RMON Long Term History List Window

---

The RMON Long Term History List window displays all the history tables that have been configured for long term monitoring. You can access this window from the Long Term History button in the [RMON History List](#) window.

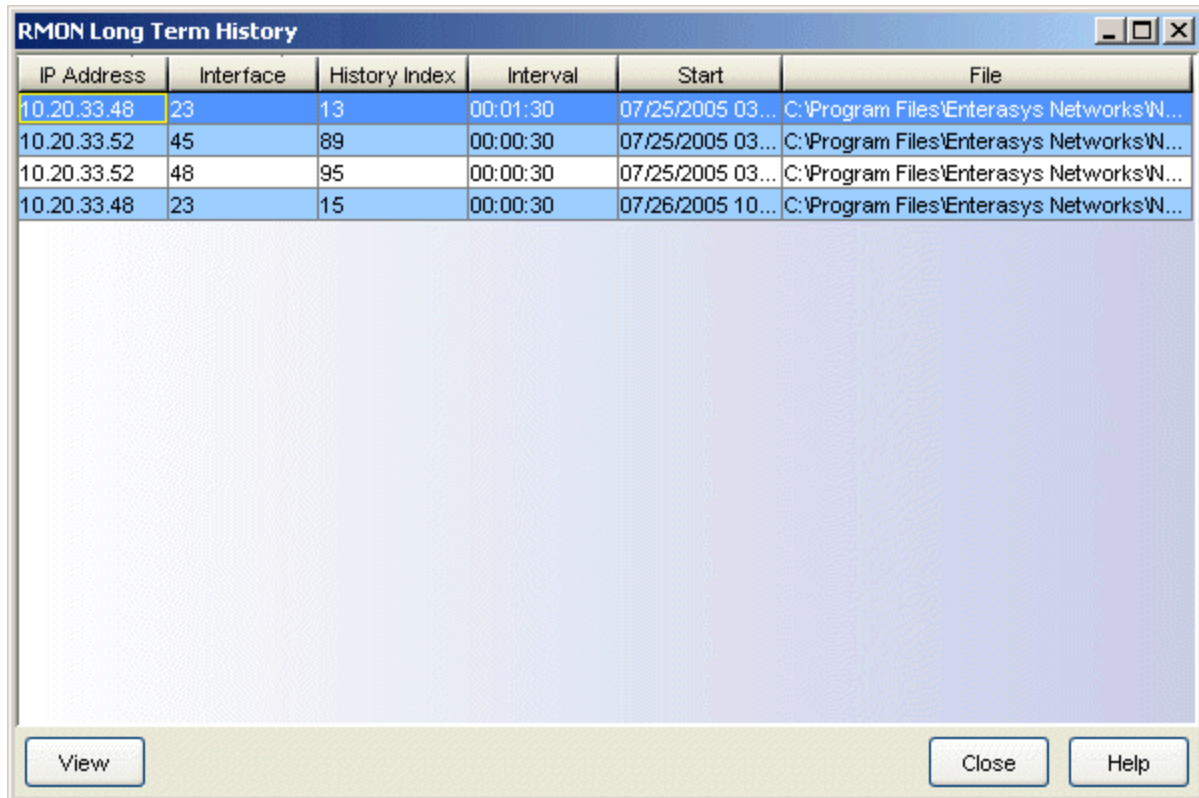
The long term history function automatically saves data from a device's history table to a comma separated variable file (\*.csv) on the client workstation. The data can then be viewed in the [RMON Long Term History](#) window, or imported into any database or spreadsheet software that accepts comma-delimited data. With the long term history function, older data is not replaced by new data. Instead, as long as the [RMON History List](#) window remains open, the .csv file on your workstation will automatically save all history data.

---

**NOTE:** The RMON Long Term History List window displays all the long term histories created on your client workstation, not just those specific to the current selected device. Only those histories created on your client workstation will be listed.

---

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.



IP Address	Interface	History Index	Interval	Start	File
10.20.33.48	23	13	00:01:30	07/25/2005 03...	C:\Program Files\Enterasys Networks\W...
10.20.33.52	45	89	00:00:30	07/25/2005 03...	C:\Program Files\Enterasys Networks\W...
10.20.33.52	48	95	00:00:30	07/25/2005 03...	C:\Program Files\Enterasys Networks\W...
10.20.33.48	23	15	00:00:30	07/26/2005 10...	C:\Program Files\Enterasys Networks\W...

**IP Address**

The device IP address.

**Interface**

The index value assigned to the port interface on the device.

**History Index**

A number that uniquely identifies the history table.

**Interval**

The time interval applicable to the table sample. For the default tables, statistical data is collected either every 30 seconds or every 30 minutes.

**Start**

The date and time the long term history was created.

**File**

The complete file path and name of the .csv file storing the data for this long term history.

### View Button

Opens the [RMON Long Term History](#) window where you can view the selected long term history file.

---

### Related Information

For information on related windows:

- [RMON History Window](#)
- [Create/Modify History Window](#)

## RMON Packet Capture

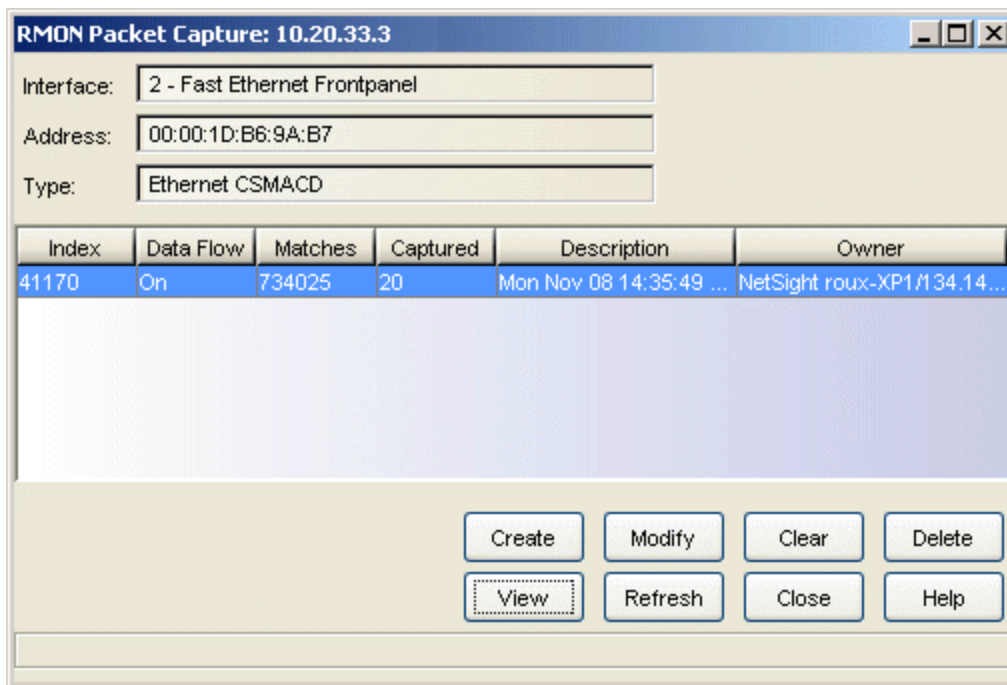
---

The RMON Packet Capture window let you configure an RMON device so that it acts like a simple network analyzer on its network segment. It provides facilities that let you manage the filters that can be used to capture packet information. The top portion of the window displays device information fields. The remainder of the window contains the Filter List and the command buttons that allow you to create, modify, clear, and delete filters, refresh the filter list, view captured packets in the [Capture Buffer](#) window.

---

**NOTE:** When the RMON Packet Capture window is initially opened the Console Event log might show several SNMP gets/sets to the selected device. This is because Console first queries RMON status on the selected device and, if it finds that RMON is disabled, Console attempts to enable it.

---



### Index

The index is a number that uniquely identifies each filter. Index numbers are automatically assigned each time a filter is created or modified; these numbers are random and will not necessarily be consecutive.

### Data Flow

Indicates the current capture status of the filter: On or Off. No packets will be captured against filters which have been turned off (although all packets will still be compared to filter parameters and matches will be counted).

### Packets Matched

Indicates the number of packets that meet the criteria set in the filter. Note that the count of matched packets displayed here does not necessarily correspond to the number of packets captured to the buffer: no packets will be captured against filters which have been turned off, and the size of each filter buffer is finite.

### Packets Captured

Indicates the number of packets (or portions of packets, as determined by the filter definition) that have been saved to the filter's buffer.

### Description

This is a user-defined text description used to identify the filter; the default description is default description.

### Owner

The owner field simply defines the owner, or originator, of the request to create a new filter; the text string entered during the filter creation process is displayed here.

---

**NOTE:** Information provided in this screen is static once it is displayed; for updated information, click **Refresh**. Creating or Modifying a filter automatically updates the list.

---

### Create Button

Opens the [Create Filter](#) window where you can define the criteria that must be met in order for a packet to be captured.

### Modify Button

Opens the [Modify Filter](#) window where you can change an existing filter to alter the criteria that must be met in order for a packet to be captured.

### Clear Button

Clears the selected filter's buffer. A filter's buffer is also cleared if a filter is modified -- or even opening the Modify window and clicking **Ok** without making any changes -- automatically clears the buffer and resets the Packets Matched counter to zero. If you confirm in the resulting *last chance* query, all packets currently stored in the filter's buffer will be deleted. If the

filter is enabled, the buffer will continue to store newly matched packets up to the configured limit.

---

**NOTE:** Clearing a filter's buffer manually does not reset the Packets Captured counter.

---

#### Delete Button

Removes one or more selected filters from the **Filters** list.

#### View Button

Opens the RMON Packet Capture window where you can view the packets that have been captured for a selected filter.

#### Refresh Button

Updates the **Filter** list.

#### Close

Dismisses the RMON Filters window.

### *Right-Click Menu*

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

---

### **Related Information**

For information on related windows:

- [RMON Alarm/Event List](#)
- [Create/Edit Alarm Window](#)
- [Create/Edit Event Window](#)

## SNMP Group Window

SNMP (Simple Network Management Protocol) facilitates the communication between a device and a network management application (such as NetSight Console) through the use of PDUs (Protocol Data Units). The management application requests data from the device by issuing Get Request or Get Next Request PDUs, or writes a new value into the device's MIB (Management Information Base) by issuing a Set Request PDU. The SNMP agent on the device responds to Gets by issuing a Get Response PDU or sends notification of unusual events to the management application by issuing a Trap PDU.

The SNMP Group window displays a summary of PDU activity and allows you to enable or disable the device's ability to issue traps. Use this window to view statistical information concerning SNMP-defined objects on your device.

To access the SNMP Group window, select **Device > MIB-II > SNMP Group** from the Device View menu bar.

The image shows a screenshot of the 'SNMP Group: 10.20.110.120' window. It is divided into two main sections: 'Errors' and 'Totals'. Each section has a table with 'Received' and 'Transmitted' columns. Below these tables are two dropdown menus: 'Calculation Mode' set to 'Poll' and 'Authentication Failure Traps' set to 'Disabled'. At the bottom right are 'Apply', 'Close', and 'Help' buttons. A 'Current Values' section is visible at the very bottom.

	Received	Transmitted
Errors		
Versions:	60	
Community Names:	128	
Community Operations:	0	
Read Only:	0	
Parse	0	
Too Big:	0	0
No Such Name:	0	1595
Bad Value:	0	0
General:	0	0

	Received	Transmitted
Totals		
Gets:	311187	
Sets:	0	
Get Requests:	97740	0
Get-Nexts:	4625	0
Get Responses:	0	102364
Set Requests:	0	0
Traps:	0	0
Messages:	102553	102364
Silent Drops:	0	
Proxy Drops:	0	

Calculation Mode: **Poll**      Authentication Failure Traps: **Disabled**

Apply    Close    Help

Current Values

## Errors Area

### Versions

Displays the total number of SNMP messages received by the SNMP agent for an unsupported SNMP version. SNMP messages include a version number, but SNMP, unlike most protocols, does not try to resolve version differences. If an SNMP agent receives a message with an unknown version number, it discards the message.

### Community Names

Displays the total number of messages received by the SNMP agent which used an SNMP community name not recognized by the agent. An SNMP Get or Set request must be accompanied by a valid community name.

### Community Operations

Displays the total number of SNMP messages received by the SNMP agent that represented an SNMP operation not allowed by the SNMP community named in the message. This means that the community name specified in the SNMP message did not have the necessary privileges to complete the operation.

### Read Only

Displays the total number of valid SNMP PDUs received by the SNMP agent which had a value of `readOnly` in the error-status field. This means that a Set operation tried to modify a variable that is not included in the SNMP community profile used for the operation. A community profile is the combination of the access mode of the community name (read-only or read-write) with the subset of MIB objects defined for the community name.

### Parse

Displays the total number of ASN.1 (Abstract Syntax Notation One) or BER (Basic Encoding Rules) errors encountered by the SNMP agent when decoding received SNMP messages. ASN.1 is the International Standards Organization (ISO) MIB-object identification and naming convention. BER is the algorithm that encodes an ASN.1 value into a form suitable for transmission. A Parse error indicates that the received BER value does not conform to the syntax rules (i.e., you received a good SNMP packet, but its data was useless).

### Too Big

Displays the total number of SNMP PDUs received/transmitted by the SNMP agent that had a value of `tooBig` in the error-status field. A Too Big



error is encountered most often when a Get-Next operation retrieves a large amount of data that cannot fit into a single SNMP message.

**No Such Name**

Displays the total number of SNMP PDUs received/transmitted by the SNMP agent that had a value of *noSuchName* in the error-status field. According to the community profile, the variable name specified in the Set command did not exist. A community profile is the combination of the access mode of the community name (read-only or read-write) with the subset of MIB objects defined for the community name.

**Bad Value**

Displays the total number of SNMP PDUs received/transmitted by the SNMP agent which had a value of *badValue* in the error-status field. This means that the incoming Set operation specified the incorrect syntax or value.

**General**

Displays the total number of SNMP PDUs received/transmitted by the SNMP agent which had a value of *genErr* in the error-status field. A General error is an error that does not fit any of the four specific error types: [Too Big](#), [No Such Name](#), [Bad Value](#), and [Read Only](#).

*Totals Area***Gets**

Displays the total number of MIB objects retrieved by the SNMP agent as the result of receiving valid SNMP Get Requests and Get-Next PDUs.

**Sets**

Displays the total number of MIB objects altered by the SNMP agent as the result of receiving valid SNMP Set Request PDUs.

**Get Requests**

Displays the total number of SNMP Get Request PDUs received (accepted and processed) and transmitted (generated) by the SNMP agent.

**Get-Nexts**

Displays the total number of SNMP Get-Next PDUs received (accepted and processed) and transmitted (generated) by the SNMP agent.

**Get Responses**

Displays the total number of SNMP Get Response PDUs received (accepted and processed) and transmitted (generated) by the SNMP agent.

**Set Requests**

Displays the total number of SNMP Set Request PDUs received (accepted and processed) and transmitted (generated) by the SNMP agent.

**Traps**

Displays the total number of SNMP Trap PDUs received (accepted and processed) and transmitted (generated) by the SNMP agent. A device cannot receive traps unless the sending-device Traps table is set up so that traps are enabled and pointed toward the IP address of the receiving station.

**Messages**

Displays the total number of messages received by the SNMP agent from the transport service and transmitted from the agent to the transport service.

**Silent Drops**

Displays the total number of Get Request, Get Next Request, Get Bulk Request, Set Request, and Inform Request PDUs received by the SNMP agent which were silently dropped because the size of a reply containing an alternate Response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.

**Proxy Drops**

Displays the total number of Get Request, Get Next Request, Get Bulk Request, Set Request, and Inform Request PDUs received by the SNMP agent which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response PDU could be returned.

**Calculation Mode**

Use the drop-down list to specify how the statistics count will be calculated:

- **Poll** -- After the completion of the current polling cycle plus one complete polling cycle, the window will display the total count of statistics processed since the device was last initialized. These totals are updated after each polling cycle.
- **Delta** -- After the completion of the current polling cycle plus two more polling cycles, the window will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.

- **Accumulate** -- After the completion of the current polling cycle plus two more polling cycles, the window will display a fresh cumulative count of statistics. This option does not clear the device counters; you can still select Poll for the total count since the device was last initialized.

**NOTE:** The SNMP Group window uses the polling intervals you have set via the NetSight Console Options window, Device Manager options.

### Authentication Failure Traps

Use the drop-down list to enable or disable the device's ability to issue traps. In order for a device to issue traps, and for the management station to receive those traps, the device's trap table must be properly configured via Local Management. See the device hardware manual for more information.

---

### Related Information

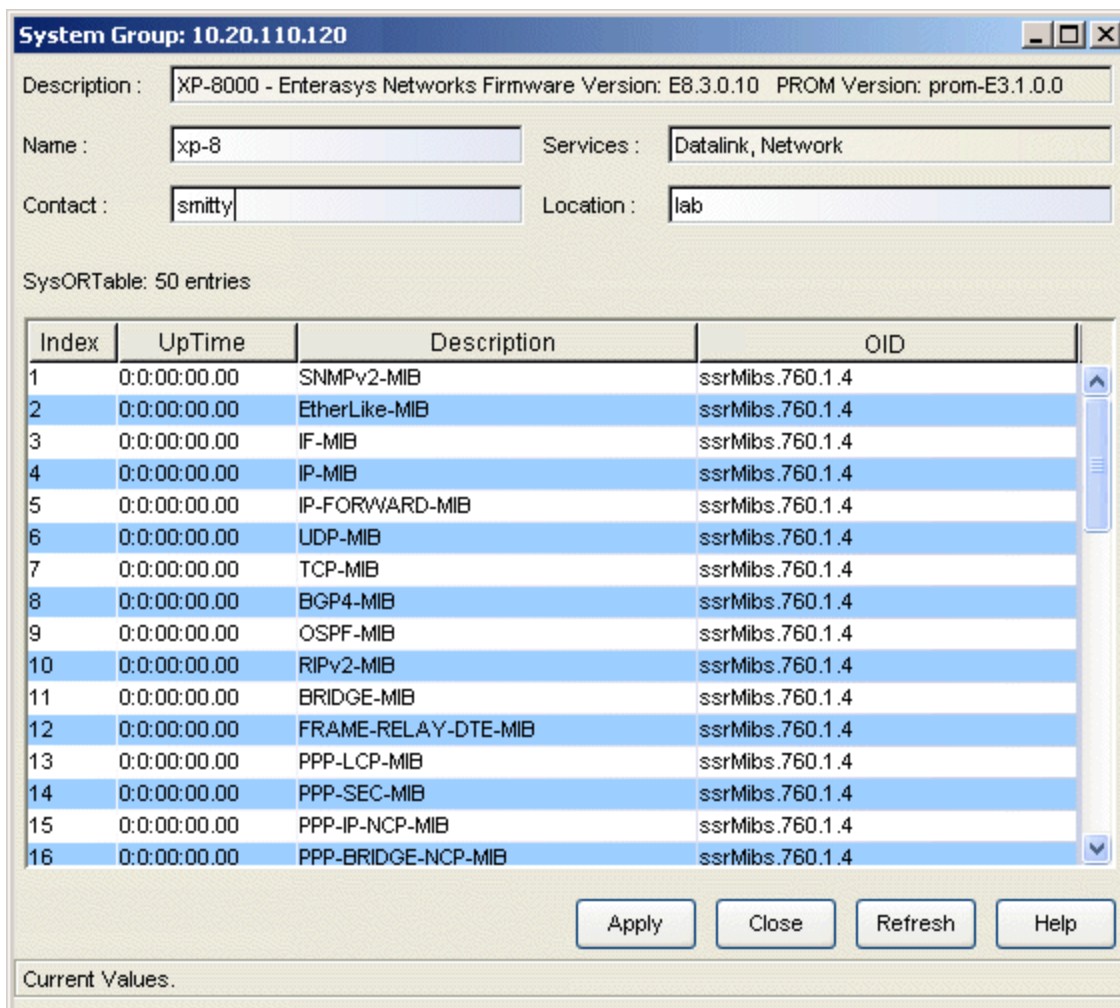
For information on related windows:

- [System Group Window](#)

## System Group Window

Use the System Group window to view and change the device name, location, and contact person. This window also includes the SysORTable which defines the Agent-Capabilities (A-C) statement for the device. An A-C statement is like formalized release notes for the device's SNMP agent. It describes what MIB modules have been implemented, and how the implementation varies from the standard.

To access the System Group window, select **Device > MIB-II > System Group** from the Device View menu bar.



**System Group: 10.20.110.120**

Description : XP-8000 - Enterasys Networks Firmware Version: E8.3.0.10 PROM Version: prom-E3.1.0.0

Name : xp-8 Services : Datalink, Network

Contact : smitty Location : lab

SysORTable: 50 entries

Index	UpTime	Description	OID
1	0:0:00:00.00	SNMPv2-MIB	ssrMibs.760.1.4
2	0:0:00:00.00	EtherLike-MIB	ssrMibs.760.1.4
3	0:0:00:00.00	IF-MIB	ssrMibs.760.1.4
4	0:0:00:00.00	IP-MIB	ssrMibs.760.1.4
5	0:0:00:00.00	IP-FORWARD-MIB	ssrMibs.760.1.4
6	0:0:00:00.00	UDP-MIB	ssrMibs.760.1.4
7	0:0:00:00.00	TCP-MIB	ssrMibs.760.1.4
8	0:0:00:00.00	BGP4-MIB	ssrMibs.760.1.4
9	0:0:00:00.00	OSPF-MIB	ssrMibs.760.1.4
10	0:0:00:00.00	RIPv2-MIB	ssrMibs.760.1.4
11	0:0:00:00.00	BRIDGE-MIB	ssrMibs.760.1.4
12	0:0:00:00.00	FRAME-RELAY-DTE-MIB	ssrMibs.760.1.4
13	0:0:00:00.00	PPP-LCP-MIB	ssrMibs.760.1.4
14	0:0:00:00.00	PPP-SEC-MIB	ssrMibs.760.1.4
15	0:0:00:00.00	PPP-IP-NCP-MIB	ssrMibs.760.1.4
16	0:0:00:00.00	PPP-BRIDGE-NCP-MIB	ssrMibs.760.1.4

Apply Close Refresh Help

Current Values.

### Description

A description of the device.

**Name**

Use this field to view or change the assigned name for the device.

**Contact**

Use this field to view or change information about the person responsible for the device.

**Services**

Displays the level of OSI (Open Systems Interconnection) service that is supported by the device:

- **Physical** -- This layer applies to the physical interface to the communications stack.
- **Datalink/Subnetwork** -- This layer applies to transmission, framing, and error control over a single communications link.
- **Network** -- This layer applies to data transfer across a network.
- **Transport** -- This layer applies to the multiplexing of data transfer across a network.
- **Session** -- This layer applies to the addition of control measures to the data exchange.
- **Presentation** -- This layer applies to the structure of the units of data that are exchanged.
- **Application** -- This layer applies to the management of communications between applications.

**Location**

Use this field to view or change a description of the physical location of the device.

*SysORTable*

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**Index**

A number used to uniquely identify a row in the table.

**Uptime**

The value of *sysUpTime* at the time this table entry was last instantiated in days:hh:mm:ss format. This value is used to help determine new entries that

have been added to the table.

**Description**

A list of the specific MIB module names that are documented in the Agent-Capabilities (A-C) Statement. The A-C Statement describes what MIB modules have been implemented on the device, and how the implementation varies from the standard.

**OID**

OID (Object Identifier) is the unique identification of the Agent Capabilities statement. The OID for the A-C statement is assigned by Extreme Networks underneath their enterprise subtree.

---

**Related Information**

For information on related windows:

- [SNMP Group Window](#)

## TCP Group Window

Use the TCP (Transmission Control Protocol) Group window to view the type of algorithm used to compute the retransmission of datagrams on your network. This window also displays the TCP connection state of the ports on your device.

To access the TCP Group window, select **Device > MIB-II > TCP Group** from the Device View menu bar

**TCP Group: 10.20.30.40**

Retransmit Algorithm: Van Jacobson

Rto. Min. [milliseconds]: 1000

Rto. Max. [milliseconds]: 64000

Maximum Connections: -1

Active Opens: 0

Passive Opens: 19

Connection Failures: 0

Closed Connection: 0

Open Connections: 0

Segments Received: 2723

Segments Transmitted: 1011

Segments Retransmitted: 1011

Incoming Seg Errors: 0

Resets: 0

TCP Connections Information

State	Local IP	Local Port	Remote IP	Remote Port
listen	0.0.0.0	23	0.0.0.0	0
listen	122.0.0.1	10000	0.0.0.0	0
listen	122.0.0.1	59231	0.0.0.0	0

Close Refresh Help

Current values.

### Retransmit Algorithm

Displays the adaptive algorithm used to determine the time-out value for retransmitting unacknowledged octets:

- **constant rto** -- Constant Retransmit Time Out.
- **MIL-STD-1778** -- MIL-STD-1778, Appendix B.
- **Van Jacobson** -- Van Jacobson algorithm.
- **other** -- None of the above.
- **unknown**

### Rto. Min. (milliseconds)

Displays the minimum amount of time (in milliseconds) that the device waits before retransmitting a segment onto the network.

### Rto. Max. (milliseconds)

Displays the maximum amount of time (in milliseconds) that the device waits before retransmitting a segment onto the network.

### Maximum Connections

Displays the maximum number of simultaneous TCP connections that the device supports. In devices where the number of connections is dynamic, the value is -1.

### Active Opens

Displays the number of times that the TCP connections transitioned to the *synSent* state from the *closed* state.

### Passive Opens

Displays the number of times that the TCP connections transitioned to the *synReceived* state from the *listen* state.

### Connection Failures

Displays the number of times that the TCP connections made a direct transition to the *closed* state from either the *synSent* state or the *synReceived* state. It also counts the number of times that the TCP connections transitioned to the *listen* state from the *synReceived* state.

### Closed Connections

Displays the number of times that the TCP connections transitioned to the *closed* state from either the *established* state or the *closeWait* state.



**Open Connections**

Displays the number of TCP connections in which the current state is either *established* or *closeWait*.

**Segments Received**

Displays the total number of segments (including those with errors), received by the device.

**Segments Transmitted**

Displays the total number of segments (including those on current connections but excluding those containing only retransmitted octets), transmitted by the device onto the network.

**Segments Retransmitted**

Displays the total number of segments (containing one or more previously-transmitted octets), retransmitted by the device onto the network. Segments are retransmitted when no segment acknowledgment is received and the retransmit timeout has not expired.

**Incoming Seg Errors**

Displays the total number of error segments received (e.g., bad TCP checksums). If this counter shows a steady increase, it may indicate that received segments have been encapsulated incorrectly.

**Resets**

Displays the number of TCP segments sent that contained the RST flag. It indicates the number of times the TCP tried to reset the connection. A reset can be caused by a faulty connection, a user request, or a lack of resources.

***TCP Connections Information***

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**State**

Displays the current state of the TCP connection: *closed*, *listen*, *synSent*, *synReceived*, *established*, *finWait1*, *finWait2*, *closeWait*, *lastAck*, *closing*, *timeWait*, or *deleteTCB*. During the course of a TCP communication session, the connection state changes depending on the current activity.

**Local IP**

Displays the local IP address for this TCP connection. When a connection is in the *listen* state and is willing to accept connections for any IP interface

associated with the device, the value 0.0.0.0 is used.

**Local Port**

Displays the local port number for this TCP connection.

**Remote IP**

Displays the remote IP address for this TCP connection.

**Remote Port**

Displays the remote port number of this TCP connection. Most TCP applications use a set of well-known ports. Well-known ports are always 256 or lower (e.g., FTP is 21, Telnet is 23, Domain Name Server is 53, etc.). Other port numbers are available for assignment as needed.

---

**Related Information**

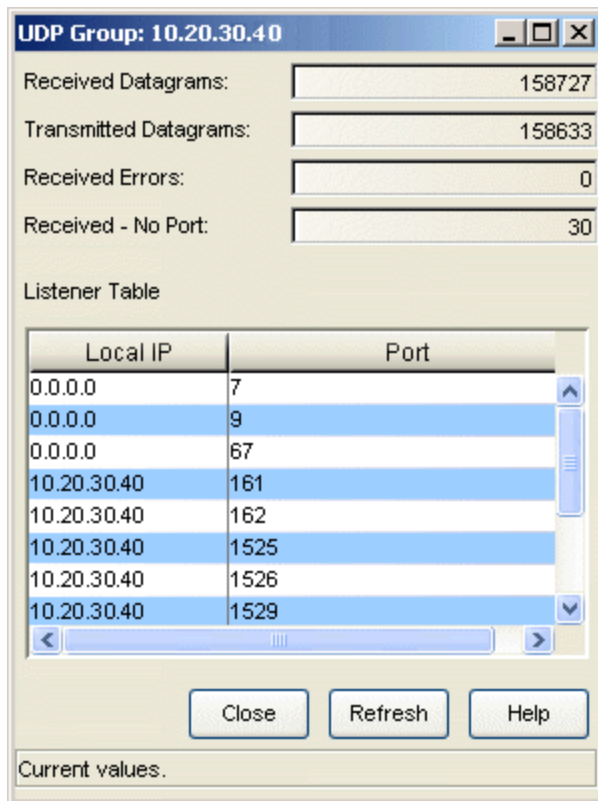
For information on related windows:

- [System Group Window](#)
- [SNMP Group Window](#)
- [UDP Group Window](#)

## UDP Group Window

Use the UDP (User Datagram Protocol) Group window to view information concerning the transport protocol for your device. The window also displays a list of UDP listeners, including their associated local IP address and port number.

To access the UDP Group window, select **Device > MIB-II > UDP Group** from the Device View menu bar.



### Received Datagrams

Displays the total number of UDP datagrams delivered to UDP users. A UDP user is the protocol port assigned by the operating system to a particular application.

### Transmitted Datagrams

Displays the total number of UDP datagrams sent from this device.

### Received Errors

Displays the number of received UDP datagrams that were not delivered (for reasons other than the lack of an application at the destination port). A

full buffer may cause Receive Errors to occur.

**Received - No Port**

Displays the total number of received UDP datagrams for which there was no application at the destination port.

*Listener Table*

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

**Local IP**

Displays the local IP address for this UDP listener. When a UDP listener accepts connections for any IP interface associated with the device, the value 0.0.0.0 is used.

**Port**

Displays the local port number for this UDP listener.

---

**Related Information**

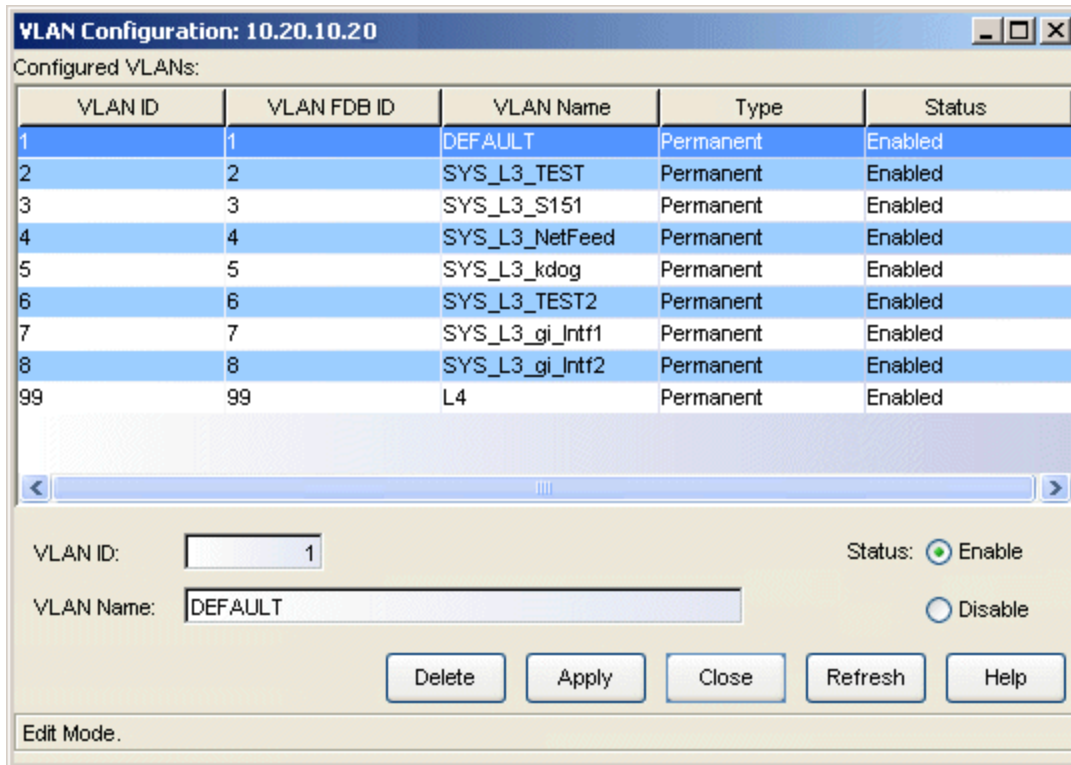
For information on related windows:

- [System Group Window](#)
- [SNMP Group Window](#)
- [TCP Group Window](#)

## VLAN Configuration Window

Use this window to add and delete VLANs (Virtual Local Area Networks), configure VLAN IDs and names, and enable or disable VLANs.

To access the VLAN Configuration window, select **Device > VLAN > VLAN Configuration** from the Device View menu bar.



The screenshot shows the 'VLAN Configuration: 10.20.10.20' window. It features a table of 'Configured VLANs' with columns for VLAN ID, VLAN FDB ID, VLAN Name, Type, and Status. Below the table are input fields for 'VLAN ID' (set to 1) and 'VLAN Name' (set to DEFAULT), along with a 'Status' section with radio buttons for 'Enable' (selected) and 'Disable'. At the bottom, there are buttons for 'Delete', 'Apply', 'Close', 'Refresh', and 'Help', and a status indicator 'Edit Mode'.

VLAN ID	VLAN FDB ID	VLAN Name	Type	Status
1	1	DEFAULT	Permanent	Enabled
2	2	SYS_L3_TEST	Permanent	Enabled
3	3	SYS_L3_S151	Permanent	Enabled
4	4	SYS_L3_NetFeed	Permanent	Enabled
5	5	SYS_L3_kdog	Permanent	Enabled
6	6	SYS_L3_TEST2	Permanent	Enabled
7	7	SYS_L3_gi_Intf1	Permanent	Enabled
8	8	SYS_L3_gi_Intf2	Permanent	Enabled
99	99	L4	Permanent	Enabled

### *Configured VLANs*

Displays information about the VLANs configured on the device. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### **VLAN ID**

Displays the unique number that identifies the selected VLAN. Allowable values range from 2 to 4094. VLAN ID 1 is reserved for the Default VLAN and cannot be used.

**VLAN FDB ID**

Displays the unique number that identifies the VLAN's Filtering Database (FDB).

**VLAN Name**

Displays the name (up to 32 characters) assigned to the VLAN.

**Type**

Displays the VLAN type: permanent (the VLAN is active and will remain so after the next reset of the device), dynamic GVRP (the VLAN is active and will remain so until removed by GVRP), or other (the VLAN is active, but is not permanent or dynamic GVRP).

**Status**

Displays the current status of the selected VLAN: Enabled (active), Disabled (not active), or Other (created but turned off or in the process of being created).

*Fields and Options***VLAN ID Field**

Enter a number that identifies a new VLAN. Allowable values range from 2 to 4094. VLAN ID 1 is reserved for the Default VLAN and cannot be used. This field is not configurable for an existing VLAN.

**VLAN Name Field**

Enter or change the name (up to 32 characters) assigned to the new or selected VLAN. It is strongly recommended that you do **not** change the name of the Default VLAN.

**Status Options**

Use the status options to enable or disable the new or selected VLAN.

**Delete Button**

Removes the selected VLAN from the Configured VLANs table and deletes the VLAN from the device.

---

**Related Information**

For information on related tasks:

- [How to Add or Modify a VLAN](#)

For information on related windows:

- [VLAN Egress Port Configuration Window](#)
- [VLAN Port Configuration \(Advanced\) Window](#)
- [VLAN Port Configuration \(Basic\) Window](#)

## VLAN Egress Port Configuration Window

---

This window displays all the VLANs configured on the device. When a VLAN is selected, the Port Egress Information field displays the ports whose egress lists contain the selected VLAN, and the egress state for each port (No Egress, Tagged, or Untagged). The window also allows you to change the egress state.

---

**NOTE:** On some devices, in order to properly configure the egress state for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via Device Manager.

---

Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

To access the VLAN Egress Port Configuration window, select **Device > VLAN > VLAN Egress Port Configuration** from the Device View menu bar.



**VLAN Egress Port Configuration: 10.20.110.120**

Selected VLAN:

VLAN ID	VLAN Name	Type	Status
1	DEFAULT	Permanent	Enabled
2	2	Permanent	Enabled
3	3	Permanent	Enabled
4	4	Permanent	Enabled
5	Q5	Permanent	Enabled

Port Egress Information:

Port	Tagging	Owner	Current	Static
1	Yes	Unknown	Unknown	Untagged
2	Yes	Unknown	Unknown	Untagged
3	Yes	Unknown	Unknown	Untagged
4	Yes	Unknown	Unknown	Untagged
5	Yes	Unknown	Unknown	Untagged
6	Yes	Unknown	Unknown	Untagged
7	Yes	Unknown	Unknown	Untagged
8	Yes	Unknown	Unknown	Untagged
9	Yes	Unknown	Unknown	Untagged
10	Yes	Unknown	Unknown	Untagged
11	Yes	Unknown	Unknown	Untagged
12	Yes	Unknown	Unknown	Untagged
13	Yes	Unknown	Unknown	Untagged
14	Yes	Unknown	Unknown	Untagged
15	Yes	Unknown	Unknown	Untagged
16	Yes	Unknown	Unknown	Untagged

Apply Close Refresh Help

Edit Mode.

### *Selected VLAN*

Displays all the VLANs configured on the device. When a VLAN is selected, the Port Egress Information field displays the ports whose egress lists contain the selected VLAN.

### **VLAN ID**

Displays the unique number that identifies the selected VLAN.

### **VLAN Name**

Displays the name (up to 32 characters) assigned to the VLAN.

**Type**

Displays the VLAN type: Permanent (the VLAN is active and will remain so after the next reset of the device), Dynamic GVRP (the VLAN is active and will remain so until removed by GVRP), or other (the VLAN is active, but is not Permanent or Dynamic GVRP).

**Status**

Displays the current status of the selected VLAN: Enabled (active), Disabled (not active), or Other (created but turned off or in the process of being created).

**Current Egress**

An octet string representing the set of ports which are transmitting traffic for this VLAN as either tagged or untagged frames.

**Current Untagged**

An octet string representing the set of ports which are transmitting traffic for this VLAN as untagged frames.

**Static Egress**

An octet string representing the set of ports which are permanently assigned to the egress list for this VLAN by management.

**Static Untagged**

An octet string representing the set of ports which should transmit egress packets for this VLAN as untagged.

*Port Egress Information*

Displays the ports whose egress lists contain the selected VLAN. Use this field to change how frames belonging to the selected VLAN will be forwarded out the port: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged). For more information see [How to Configure Port Egress State](#).

**Port**

Displays the number that identifies the port.

**Tagging**

Displays whether the port is implementing the 802.1Q VLAN functionality of tagging frames and GVRP (GARP VLAN Registration Protocol).

**Owner**

Specifies how the port's egress state was configured: by management, by GVRP (GARP VLAN Registration Protocol), or by Dynamic Egress.

### Current

Displays the current egress state for the port. The egress state specifies how frames belonging to the selected VLAN are forwarded out the port: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged).

### Static

Displays the desired egress state for the port: No Egress (frames will not be transmitted), Tagged (frames will be transmitted as tagged), or Untagged (frames will be transmitted as untagged). Right-mouse click on the port to select the desired egress state from the menu.

---

**NOTES:** On the X-Pedition Router, Access ports cannot be set to tagged, and Trunk ports cannot be set to untagged. Egress state cannot be set by the user on X-Pedition Routers with firmware versions of E8.1.0.0 or earlier.

On some devices, in order to properly configure the egress state for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via Device Manager.

---

## Related Information

For information on related tasks:

- [How to Configure Port Egress State](#)

For information on related windows:

- [VLAN Configuration Window](#)
- [VLAN Port Configuration \(Advanced\) Window](#)
- [VLAN Port Configuration \(Basic\) Window](#)

## VLAN Port Configuration (Advanced) Window

Use this window to configure advanced VLAN port parameters such as Ingress Filtering and GVRP Status. You can also access basic VLAN port parameters from this window.

Access the VLAN Port Configuration (Advanced) window from the VLAN Port Configuration (Basic) window. In the Device View, select **Device > VLAN > VLAN Port Configuration** from the menu bar. In the [VLAN Port Configuration \(Basic\) window](#) click the **Advanced** button to open the VLAN Port Configuration (Advanced) window

The screenshot shows the 'VLAN Port Configuration [Advanced]: 10.20.110.120' window. It features a table titled 'Current Port Configuration Information:' with columns: Port, Port VLAN ID, VLAN Name, Owner, Port Operational Mode, Current Egress State, Static Egress State, Acceptable Frame Types, Ingress Filtering, GVRP Status, GVRP Failed Registration, and GVRP Last. Below the table are configuration fields for 'Port VLAN ID (Name)', 'VLAN Type / Status', 'Current Egress State', and 'Egress State'. On the right, there are dropdown menus for 'Acceptable Frame Types', 'Ingress Filtering', and 'GVRP Status'. At the bottom right are buttons for 'Basic...', 'Apply', 'Close', 'Refresh', and 'Help'.

Port	Port VLAN ID	VLAN Name	Owner	Port Operational Mode	Current Egress State	Static Egress State	Acceptable Frame Types	Ingress Filtering	GVRP Status	GVRP Failed Registration	GVRP Last
1	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Enabled	Enabled	0	00-00-00-00
2	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
3	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Enabled	Disabled	0	00-00-00-00
4	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
5	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
6	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
7	1	DEFAULT	Unkn...	Untagged	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
8	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Enabled	Disabled	0	00-00-00-00
9	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
10	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Enabled	0	00-00-00-00
11	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Enabled	0	00-00-00-00
12	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Enabled	0	00-00-00-00
13	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00
14	1	DEFAULT	Unkn...	Hybrid	Unknown	Untagged	No Capability	Disabled	Disabled	0	00-00-00-00

### Current Port Configuration Information

This table displays the advanced VLAN parameters configured for each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

#### Port

Displays the number that identifies the port.

#### Port VLAN ID

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

for the port. Endpoints connected to the port become members of that VLAN. All untagged frames received on the port are tagged with the PVID, unless a classification rule exists for the frame's classification type.

**VLAN Name**

Displays the name (up to 32 characters) assigned to the VLAN.

**Owner**

Specifies how the port's Egress State was configured: by management, by GVRP (GARP VLAN Registration Protocol), or by Dynamic Egress.

**Port Operational Mode**

Displays the port's operational mode:

- **DTrunk** -- the port's Egress State (for all VLANs) is Untagged and its Acceptable Frame Type setting is Accept All
- **QTrunk** -- the port's Egress State (for all VLANs) is Tagged and its Acceptable Frame Types setting is Accept Tagged
- **Tagged** -- the port's Egress State (for the VLAN designated as its PVID) is Tagged
- **Hybrid** -- the port's Egress State (for the VLAN designated as its PVID) is Untagged, its Egress State (for the remaining VLANs) is No Egress, and its Acceptable Frame Types setting is Accept All
- **Untagged** -- the port's Egress State (for the VLAN designated as its PVID) is Untagged
- **NoEgress** -- the port's Egress State (for the VLAN designated as its PVID) is No Egress
- **Unknown** -- the port's operational mode is none of the above

---

**NOTE:** For the X-Pedition Router, port operational modes are:

- **Access Port** -- the port's Acceptable Frame Types is Accept All, its Egress State is Untagged, and its PVID can be any VLAN.
- **Trunk Port** -- the port's Acceptable Frame Types is Accept Tagged, its Egress State is Tagged, and its PVID is the Default VLAN.

---

**Current Egress State**

Displays the current egress (forwarding) state for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

### Static Egress State

Displays the desired egress (forwarding) state for the port, No Egress, Tagged, or Untagged, as selected using the drop-down list in the Egress State field at the bottom of the window.

---

**NOTES:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

The Static Egress State will not update until you click the **Apply** button.

---

### Acceptable Frame Types

Displays a port's Acceptable Frame Types setting: Accept All (the port accepts both tagged and untagged frames), Accept Tagged (the port accepts only tagged frames) or No Capability (the port does not support this functionality).

### Ingress Filtering

Displays whether the port is performing Ingress Filtering. Ports performing Ingress Filtering will discard any frame received whose VLAN classification is not on the port's egress list.

### GVRP Status

Displays whether GVRP (GARP VLAN Registration Protocol) is currently enabled or disabled on the port. GVRP is a protocol used to dynamically add VLANs to port egress lists across a domain. Ports that do not support this functionality will display N/A.

### GVRP Failed Registration

Displays the total number of failed GVRP registrations for all VLANs on the port. Ports that do not support this functionality will display N/A.

### GVRP Last PDU

Displays the source MAC Address of the last GVRP message (PDU, Protocol Data Unit) received on the port. Ports that do not support this functionality will display N/A.

## *Fields and Options*

### Port VLAN ID [Name] Field

Use this drop-down list to select the VLAN you want to assign as the PVID (Port VLAN ID) for the selected port.

---

**NOTE:** On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

---

### VLAN Type/Status

Displays the Type (Permanent, Dynamic GVRP, or other) and Status (Enabled, Disabled, or other) for the VLAN selected in the Port VLAN ID [Name] field. See the [VLAN Configuration window](#) for more information.

### Current Egress State

Displays the current Egress State for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

### Egress State Field

Use the drop-down list to specify the Egress State for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

---

**NOTES:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

On some devices, in order to properly configure the Egress state for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via Device Manager.

---

### Acceptable Frame Types Field

Use the drop-down list to specify the Acceptable Frame Types state for the selected port: Accept All (the port accepts both tagged and untagged frames), or Accept Tagged (the port accepts only tagged frames). If the port does not support this functionality, the field will be grayed out.

---

**NOTE:** On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.

---

### Ingress Filtering Field

Use the drop-down list to specify whether the port will perform Ingress Filtering: Enable or Disable. Ingress Filtering determines if a frame is eligible to be forwarded based on whether the VLAN associated with the frame is on the receiving port's Egress List.

---

**NOTE:** On the X-Pedition Router, Ingress Filtering is always enabled and cannot be disabled.

---

### GVRP Status Field

Use the drop-down list to specify whether GVRP (GARP VLAN Registration Protocol) will be enabled on the port. GVRP is a protocol used to dynamically add VLANs to port egress lists across a domain. If the device does not support GVRP, this field will be grayed out.

### Basic Button

Click **Basic** to access the [VLAN Port Configuration \(Basic\)](#) window.

---

### Related Information

For information on related windows:

- [VLAN Configuration Window](#)
- [VLAN Egress Port Configuration Window](#)
- [VLAN Port Configuration \(Basic\) Window](#)



## VLAN Port Configuration (Basic) Window

Use this window to configure basic VLAN port parameters such as VLAN name, Egress State, and Acceptable Frame Types. You can also access advanced VLAN port parameters from this window.

To access the VLAN Port Configuration (Basic) window, select **Device > VLAN > VLAN Port Configuration** from the Device View menu bar.

**VLAN Port Configuration [Basic]: 10.20.30.40**

Current Port Configuration Information:

Port	Port VLAN ID	VLAN Name	Port Operational Mode	Egress State	Acceptable Frame Types
1	1	DEFAULT VLAN	Untagged	Untagged	Accept All
2	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
3	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
4	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
5	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
6	2		No Egress	No Egress	Accept All
7	1	DEFAULT VLAN	No Egress	No Egress	Accept All
8	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
9	1	DEFAULT VLAN	Tagged	Tagged	Accept All
10	1	DEFAULT VLAN	No Egress	No Egress	Accept All
11	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
12	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
13	1	DEFAULT VLAN	Hybrid	Untagged	Accept All
14	1	DEFAULT VLAN	Hybrid	Untagged	Accept All

Port VLAN ID(Name): 1 [DEFAULT VLAN]

VLAN Type / Status: Permanent / Enabled

Current Egress State: Untagged

Egress State: Untagged

Acceptable Frame Types: Accept All

Advanced... Apply Close Refresh Help

Edit Mode.

### *Current Port Configuration Information*

This table displays the basic VLAN parameters configured for each port. Console provides table options and tools that let you customize table settings and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

### Port

Displays the number that identifies the port.

### Port VLAN ID

Displays the VLAN ID of the VLAN assigned to the port. When you assign a VLAN to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port. Endpoints connected to the port become members of that VLAN. All untagged frames received on the port are tagged with the PVID, unless a classification rule exists for the frame's classification type.

### VLAN Name

Displays the name (up to 32 characters) assigned to the VLAN.

### Port Operational Mode

Displays the port's operational mode:

- **DTrunk** -- the port's Egress State (for all VLANs) is Untagged and its Acceptable Frame Type setting is Accept All
- **QTrunk** -- the port's Egress State (for all VLANs) is Tagged and its Acceptable Frame Types setting is Accept Tagged
- **Tagged** -- the port's Egress State (for the VLAN designated as its PVID) is Tagged
- **Hybrid** -- the port's Egress State (for the VLAN designated as its PVID) is Untagged, its Egress State (for the remaining VLANs) is No Egress, and its Acceptable Frame Types setting is Accept All
- **Untagged** -- the port's Egress State (for the VLAN designated as its PVID) is Untagged
- **NoEgress** -- the port's Egress State (for the VLAN designated as its PVID) is No Egress
- **Unknown** -- the port's operational mode is none of the above

---

**NOTE:** For the X-Pedition Router, port operational modes are:

- **Access Port** -- the port's Acceptable Frame Types is Accept All, its Egress State is Untagged, and its PVID can be any VLAN.
  - **Trunk Port** -- the port's Acceptable Frame Types is Accept Tagged, its Egress State is Tagged, and its PVID is the Default VLAN.
- 

### Egress State

Displays the current Egress State for the port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

---

**NOTE:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

---

### Acceptable Frame Types

Displays a port's Acceptable Frame Types setting: Accept All (the port accepts both tagged and untagged frames), Accept Tagged (the port accepts only tagged frames) or No Capability (the port does not support this functionality).

### *Fields and Options*

#### Port VLAN ID [Name] Field

Use this drop-down list to select the VLAN you want to assign as the PVID (Port VLAN ID) for the selected port.

---

**NOTE:** On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

---

#### VLAN Type/Status

Displays the Type (Permanent, Dynamic GVRP, or other) and Status (Enabled, Disabled, or other) for the VLAN selected in the Port VLAN ID [Name] field. See the [VLAN Configuration window](#) for more information.

#### Current Egress State

Displays the current Egress State for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

#### Egress State Field

Use the drop-down list to specify the Egress State for the selected port: No Egress (frames are not forwarded out the port), Tagged (only tagged frames are forwarded out the port), Untagged (only untagged frames are forwarded out the port).

---

**NOTES:** On the X-Pedition Router, the Egress State is configured automatically by the device according to the [Acceptable Frame Types](#) state.

On some devices, in order to properly configure the Egress State for backplane ports, the Auto VLAN Backplane Configuration option should be set to disabled. This option is available via local management. If the option is set to enabled, the backplane ports cannot be set to No Egress via Device Manager.

---

#### Acceptable Frame Types Field

Use the drop-down list to specify the Acceptable Frame Types state for the selected port: Accept All (the port accepts both tagged and untagged frames), or Accept Tagged (the port accepts only tagged frames). If the port does not support this functionality, the field will be grayed out.

---

**NOTE:** On the X-Pedition Router, if the Acceptable Frame Types state is set to Accept Tagged, then the device automatically sets the Egress State to Tagged. If the Acceptable Frame Types state is set to Accept All, then the Egress State is automatically set to Untagged. In addition, if the Acceptable Frame Types state is set to Accept Tagged, then the port automatically becomes a Trunk port with the Default VLAN as its PVID. If you want to specify a VLAN other than the Default VLAN as the PVID, you must set the Acceptable Frame Types state to Accept All.

---

#### Advanced Button

Opens the [VLAN Port Configuration \(Advanced\) window](#).

---

#### Related Information

For information on related windows:

- [VLAN Configuration Window](#)
- [VLAN Egress Port Configuration Window](#)
- [VLAN Port Configuration \(Advanced\) Window](#)

# RoamAbout Wireless Manager Help

---

RoamAbout Wireless Manager is a comprehensive tool that provides network management for Wireless RoamAbout Access Points and RoamAbout R2 devices. Using RoamAbout Wireless Manager, you can view management information for R2, AP3000, and AP4102 devices. In addition, for AP4102 devices, RoamAbout Wireless Manager lets you configure individual device settings and create templates for global device configuration. RoamAbout Wireless Manager also lets you easily monitor 802.11 statistics and error statistics in both line graph and table format.

## Features and Functionality

### Configure AP4102 Devices

RoamAbout Wireless Manager provides the ability to configure individual AP4102 devices via the Element Configuration window. Configuration settings are organized into the following areas:

- Device identification (sysName, sysDescr, sysLocation)
- RADIUS server settings for the device's primary and secondary RADIUS servers
- Scan settings for rogue detection
- Authentication settings
- CDP global and port settings
- Filter Control configuration
- Radio A and B/G configuration

When you are ready to apply the settings to the device, you have the ability to choose which of the settings will be applied by enabling or disabling the appropriate sections. For more information, see [How to Configure a Device](#).

### Create Configuration Templates for your AP4102 Devices

The AP Templates tool lets you create your own library of customized AP configuration templates that you can then apply globally to your AP4102 devices. Templates can configure the same settings as those listed above for device configuration (with a few exceptions of settings that cannot be globally applied). With RoamAbout Wireless Manager you can:

- Create multiple templates, each with its own purpose. For example, you could create one template for authentication settings and another for filter control settings. Or you could create one template for one group of devices and another template for a second group of devices. You control what settings are applied to devices by enabling or disabling portions of the template.
- Create a template based on a current device configuration.
- Compare current device settings with template settings and then apply templates to devices.

For more information, see [How to Create and Apply Templates](#).

### View AP Settings (Right-Panel Tabs)

RoamAbout Wireless Manager right-panel tabs let you quickly view AP3000 and AP4102 device configuration settings:

- Device Information
- AP Interface Configuration
- AP Interface Security Configuration
- AP Client List
- AP Neighbor List
- Neighbor Scan Settings
- RADIUS Server Settings

For more information, see [How to View AP Configuration Settings](#).

### View R2 Settings (Right-Panel Tabs)

RoamAbout Wireless Manager right-panel tabs let you quickly view RoamAbout R2 device configuration settings.

- Device Information
- R2 Wireless Configuration Settings
- R2 Management Information
- R2 Miscellaneous Controls
- R2 Error Log Information

For more information, see [How to View R2 Configuration Settings](#).

### Statistics Monitoring

Monitor 802.11 statistics and error statistics for the active interfaces on one or more devices using the AP Statistics Monitor and the AP Error Statistics Monitor windows. Statistics can be viewed as line graphs or in a table format. In addition, RoamAbout Wireless Manager provides options and

tools that let you easily view, save, print, and export the graphs and tables. For more information, see [How to Monitor Statistics](#).

## Main Window

---

The RoamAbout Wireless Manager main window is divided into a left-panel device tree, right-panel tabs, and an Event View. The device tree displays only the managed wireless devices in your network. The devices are organized just as they are in the Console device tree. You must add or delete wireless devices through Console. The right-panel tabs display detailed information about the device or device group selected in the device tree. The Event View displays alarm and event information for RoamAbout Wireless Manager. RoamAbout Wireless Manager events are also displayed in the Console Event View.

---

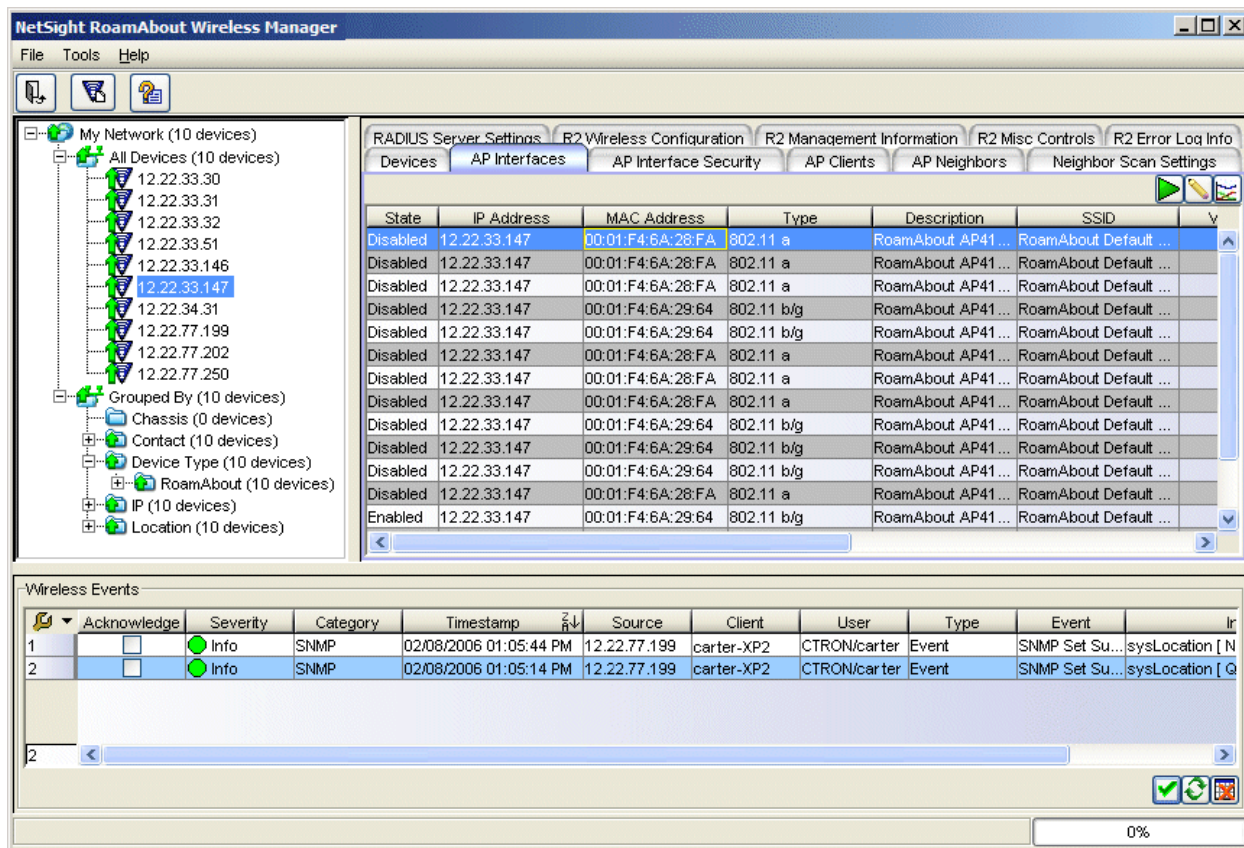
**TIP:** Use the table options and tools to find, filter, sort, print, and export information in RoamAbout Wireless Manager tables, and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.

---

Information on the Main window features:

- [Menu Bar](#)
- [Toolbar](#)
- [Event View](#)





## Menu Bar

The menu bar on the RoamAbout Wireless Manager main window provides access to RoamAbout Wireless Manager functions. For information on menu options available from right-click menus, see [Right-click Menu Options](#).

### File Menu

#### File > Exit

Exits the RoamAbout Wireless Manager application. This menu option serves the same function as the **Exit** button on the toolbar.

### Tools Menu

#### Tools > AP Templates

Opens the Wireless Templates window where you can create and edit your AP Templates. This menu option serves the same function as the **AP Templates** button on the toolbar.

## *Help Menu*

### **Help > Help Topics**

Opens the RoamAbout Wireless Manager Help system.

### **Help > About This Window**

Displays information about the currently selected right-panel tab.

## *Right-click Menu Options*

The following menu options are only available from right-click menus.

### **AP Statistics Monitor**

Launches the [AP Statistics Monitor window](#) where you can monitor 802.11 statistics for the active interfaces on the selected devices.

### **AP Error Statistics Monitor**

Launches the [AP Error Statistics Monitor window](#) where you can monitor 802.11 error statistics for the active interfaces on the selected devices.

### **Configure Device**

Opens the [Configure Device window](#) where you can configure the settings of an individual AP4102 device.

### **Compare to Template**

Launches the [AP Template Wizard](#) that lets you compare the current configuration settings on selected devices to a template and then apply the template settings to those devices.

### **Table Tools**

Use the table options and tools to find, filter, sort, print, and export information in RoamAbout Wireless Manager tables, and customize table settings.

---

## **Related Information**

For information on related windows:

- [Main Window](#)
- [Toolbar](#)

## Toolbar

---

The toolbar on the RoamAbout Wireless Manager main window provides easy access to certain RoamAbout Wireless Manager functions.



### Exit

Exits the RoamAbout Wireless Manager application. This button serves the same function as the **File > Exit** menu option.

### AP Templates

Opens the Wireless Templates window where you can create and edit your AP Templates. This button serves the same function as the **Tools > AP Templates** menu option.

### Help

Launches the RoamAbout Wireless Manager Help, and displays information about the currently selected right-panel tab. This button serves the same function as the **Help > About This Window** menu option.

---

## Related Information

For information on related windows:

- [Main Window](#)
- [Menu Bar](#)

## Event View

---


The Event View at the bottom of the RoamAbout Wireless Manager main window displays error and informational messages about RoamAbout Wireless Manager events. (RoamAbout Wireless Manager events are also displayed in the Console Event View.) The view displays the most recent 10,000 entries in the log file. The current log file is automatically archived when its size reaches 5 megabytes and a new log file is opened. Use the Event Logs view in the Console Options window to configure the number of event logs to save and the number of entries to display in the table.

Wireless Events										
	Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event	
1	<input type="checkbox"/>	Info	SNMP	01/31/2006 03:01:22 PM	10.20.33.30	carter-XP2	CTRON/carter	Event	SNMP Set Failed: Device Timeout	
2	<input type="checkbox"/>	Info	SNMP	01/31/2006 03:03:52 PM	10.20.33.31	carter-XP2	CTRON/carter	Event	SNMP Set Failed: Device Timeout	

2

0%

### 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.

### Timestamp

The date and time when the event occurred.

### Source

The IP address of the host that was the source of the event.

### 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 event.



### Show/Hide Acknowledged Events Button

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


**Refresh Button**

Refreshes the log.

**Clear Current View Button**

Clears entries from the current table.

### *Right-click Menu Options*

The event log right-click menu lets you *Acknowledge* and *Unacknowledge* events and open an *Event Details* window that shows additional information about an event selected in the Event Log. It also provides options and a standard set of table tools to help you find, filter, sort, print, and export information in a table and customize table settings. You can access the menu options 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). For more information, see Table Tools.

---

### **Related Information**

For information on related windows:

- [RoamAbout Wireless Manager Main Window](#)

## How To Use RoamAbout Wireless Manager

---





The **How To** help section contains help topics that give you instructions for performing tasks in RoamAbout Wireless Manager.

## How to Configure a Device

---

Use RoamAbout Wireless Manager to configure the settings of an individual AP4102 device. If desired, you can save the configuration as a template that you can then apply to other devices. Only AP4102 devices are configurable.

1. In the RoamAbout Wireless Manager device tree, right-click on an AP4102 device and select **Configure Device**. The Element Configuration window opens.
2. The left panel lists all the configurable components for the device. Select the desired nodes and configure the settings. Click the **Refresh** button if you would like to re-display the settings on the device rather than any changes you have made.

**NOTE:** Only settings from enabled nodes will be written to the device. A disabled node has a red X () on it. Use the toolbar buttons to enable or disable an individual node , a node group , or all nodes . You can use this functionality when configuring a device to make sure that you are only setting the desired values, by disabling all nodes except the desired node.

3. If you would like to save this device configuration as a template, click **Save As Template** and enter a template name. The template will now be listed in the Wireless Templates window (Tools > AP Templates) and can be applied to other devices. Again, you can use the enable/disable node functionality (see Note above) to specify which components you want that template to configure. Only enabled nodes will be set on devices when you apply the template to devices.

**NOTE:** When you save a configuration as a template, the password fields in the template will not have the actual value of the password, but rather "\*\*\*\*\*". If you want the template to configure the passwords, you will need to [edit the template](#) so that the password fields have the actual values.

4. Click **Apply** or **OK** to set the configuration on the device. (**Apply** will leave the Element Configuration window open when the set is complete; **OK** will close the window.) A Configuration Progress window opens, showing you the status of the configuration set. You can double-click on a row in the Configuration Progress window to see further details. Click **OK** to close the window.

## **Related Information**

For information on related tasks:

- [How to Create and Apply AP Templates](#)



## How to Create and Apply AP Templates

---

The RoamAbout Wireless Manager AP Templates tool lets you create your own library of customized AP configurations that you can then easily apply to your AP4102 network devices. A template is like a ready-made configuration that can be used over and over again for multiple devices. With templates, you can quickly configure APs that have the same configuration requirements. For example, let's say devices A, B, and C all use the same RADIUS server settings. Using the AP Templates tool, you can create one template with those RADIUS server settings and apply it to all three devices. This saves you from having to do three individual device configurations. In addition, you can use the template whenever you add a new device.


Instructions on:


- [Creating a Template](#)
- [Editing a Template](#)
- [Deleting a Template](#)
- [Applying a Template to Devices](#)

### *Creating a Template*

There are two ways to create a template. You can either create a new template or you can create a template from an existing device configuration by saving that configuration as a template.

#### Creating a New Template:

1. From the RoamAbout Wireless Manager menu bar, select **Tools > AP Templates**, or select the AP Templates button  in the RoamAbout Wireless Manager toolbar. The Wireless Templates window opens.
2. Click the **New** button. The Template Configuration window opens.
3. Enter the Template Name and Description.
4. In the left-panel tree, you will see listed all the configurable components of a template. Enable the node or nodes that you want to configure. Select each node and configure the settings as desired.

**NOTE:** When you create a template, you can pick and choose which components you want that template to configure by enabling or disabling individual components (nodes) in the left-panel tree. Only enabled nodes will be set on devices when you apply the template to devices. This allows you to create templates for different uses. For example, you could have one template for RADIUS server settings, and another template for security settings. A disabled node has a red X () on it. Use the toolbar buttons to enable or disable an individual node

, a node group , or all nodes .

5. When you have completed configuring the template, click **Save**. The template will be listed in the Wireless Templates window.
6. Use the [AP Template wizard](#) to compare selected devices to the template, and apply the template to those devices.


### Saving a Device Configuration as a Template:

1. In the RoamAbout Wireless Manager device tree, right-click on an AP4102 device and select **Configure Device**. The Element Configuration window opens. You can use the enable/disable node functionality ([see Note above](#)) to specify which components you want that template to configure. Only enabled nodes will be set on devices when you apply the template to devices.
2. Click **Save As Template** and enter a template name. Click **OK**. The template will now be listed in the Wireless Templates window (Tools > AP Templates).

**NOTE:** When you save a configuration as a template, the password fields in the template will not have the actual value of the password, but rather "\*\*\*\*\*". If you want the template to configure the passwords, you will need to [edit the template](#) so that the password fields have the actual values.

### Editing a Template


Use the following steps to make changes to an existing template.

1. From the RoamAbout Wireless Manager menu bar, select **Tools > AP Templates**, or select the AP Templates button  in the RoamAbout Wireless Manager toolbar. The Wireless Templates window opens.
2. Select the desired template and click **Edit**. The Template Configuration window opens.
3. Make any desired changes to the template and click **Save**.

4. Use the [AP Template wizard](#) to compare selected devices to the template, and apply the template to those devices.

### *Deleting a Template*

Use the following steps to delete a template.

1. From the RoamAbout Wireless Manager menu bar, select **Tools > AP Templates**, or select the AP Templates button  in the RoamAbout Wireless Manager toolbar. The Wireless Templates window opens.
2. Select the desired template and click **Delete**.
3. Click **Ok**.

### *Applying a Template to Devices*

Use the AP Template Wizard to compare the current configuration settings on selected devices to a template and then apply the template settings to those devices.

1. In the RoamAbout Wireless Manager left-panel device tree, right-click on one or more devices or a device group, and select **Compare to Template**.
2. The AP Template Wizard opens, and displays the devices you have selected. Configurable devices (AP4102) are displayed in the left panel, and non-configurable devices (AP3000, RoamAbout R2, and devices without read-write access) are displayed in the right panel. Click **Next**.
3. Select the template you want to compare the devices to. Click **Next**.
4. The wizard displays the differences between the current settings on each device and the template settings. (Only configuration values for [enabled nodes](#) on the template will be compared.) Double-click an entry to open a Details window that lists each setting, and the old (current) value on the device and the new value that will be applied with the template. Click **Next**.
5. The wizard displays the devices that the template will be applied to. Click the **Finish** button to apply the template to those devices.

---

### **Related Information**


For information on related tasks:

- [How to Configure a Device](#)

## How to Monitor AP Statistics

---

RoamAbout Wireless Manager lets you monitor 802.11 statistics and error statistics for the active interfaces on one or more devices using the AP Statistics Monitor and the AP Error Statistics Monitor windows.

To access these window, right-click on the desired devices in the device tree and select either **AP Statistics Monitor** or **AP Error Statistics Monitor**. You can also access the AP Statistics Monitor from certain right-panel tabs by selecting an interface and clicking the Monitor button  in the upper right-hand corner of the tab.

AP statistics can be viewed as line graphs (using the Packet Statistics tab) or in a table format (using the Data Table tab). In addition, RoamAbout Wireless Manager provides options and tools that let you easily view, save, print, and export the graphs and tables.

Information on:

- [Packet Statistics Tab](#)
  - [Line Graph Tools](#)
- [Data Table Tab](#)
  - [Table Tools](#)

### *Packet Statistics Tab*

Selecting the **Packet Statistics** tab displays the AP statistics in a line graph format. You can display statistics for one or multiple devices depending on your selection in the device tree. The chart legend displays the line color that corresponds to each device interface.

At the top of the window, select the desired settings depending on how you want to display the graph information. First, select how you want the data displayed:

- **Raw** - plots the data as the accumulated value obtained during the selected poll interval.
- **Rate** - plots the data as a value per second.
- **Delta** - plots the data as the accumulated value that is the amount of the change from the preceding value, per selected poll interval.

Then, set the poll rate and maximum number of samples:

- **Poll Rate (seconds)** - Specifies the interval between polling the selected devices for information. The frequency must be set to a non-zero value. To change the value, enter a number and click the **Set** button.
- **Maximum # of Samples** - configures the maximum number of samples to show at one time in the graphs. To change the value, enter a number and click the **Set** button.

### *Line Graph Tools*

RoamAbout Wireless Manager provides line graph options and tools that let you customize the graph, and save, print, and zoom in to the graph. You can access these tools by right-clicking on a graph and selecting an option from the menu. In addition, double-clicking on a graph opens a Detail window that presents an enlarged display of the graph for easier viewing of data.

### **Right-Click Menu Options**

Right-click on an individual graph to see the following options:

- **Properties** - opens the Chart Properties window where you can custom-design the look of the line graph and also add a legend specifically for that graph.
- **Save As** - lets you save the graph in .png format.
- **Print** - lets you print the graph.
- **Zoom In** - zoom in on one or both axes.
- **Zoom Out** - zoom out on one or both axes.
- **Auto Range** - set one or both axes back to the default range.

### **Open a Detail Window**

Double-click on an individual graph to open a Detail window that presents an enlarged graph that allows easier viewing of data, as well as the ability to export, print, and save one specific graph. All right-click menu options are available from this window as well.

### **Export Line Graphs**

Click the **Export** button at the bottom of the statistics window (or Detail window) to export the line graph or graphs as a .pdf file.

### **Pause/Restart Chart Polling**



Lets you pause or restart polling for all the line graphs (and the data table), or for an individual line graph in the Detail window. This lets you freeze the graph data so that you can easily print, save, or export the desired data.

## Print Charts

Click the **Print** button at the bottom of the statistics window (or Detail window) to print the contents of the window.

## *Data Table Tab*

Selecting the **Data Table** tab displays the AP statistics in a table format. You can display statistics for one or multiple devices depending on your selection in the device tree. The Data Table displays raw data as retrieved from the device.

At the top of the window, only the poll rate setting applies to the Data Table:

- **Poll Rate (seconds)** - Specifies the interval between polling the selected devices for information. The frequency must be set to a non-zero value. To change the value, enter a number and click the **Set** button.

## *Table Tools*

RoamAbout Wireless Manager provides table options and tools that let you customize table properties, and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right-mouse click on a column heading or anywhere in the table body.

## Right-Click Menu Options

Right-click on a column heading or anywhere in the table body to see the following options:

- **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.
- **Auto Export** - places the Auto Export toolbar at the top of the table
- **Select All** - selects all of the entries in the table.
- **Table Tools**
  - **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.

### Export Table

Click the **Export** button at the bottom of the Statistics window (or Detail window) to export the table as a .pdf file.

### Pause/Restart Chart Polling



Lets you pause or restart polling for the data table (and for all the packet statistics graphs). This lets you freeze the table data so that you can easily print, save, or export the desired data.

### Print Table

Click the **Print** button at the bottom of the statistics window to print the contents of the window.

## How to Set RoamAbout Wireless Manager Options

---

The RoamAbout Wireless Manager options let you select which right-panel tabs you want displayed in the RoamAbout Wireless Manager window. Use the Console Options window (**Tools > Options** in the Console menu bar) to set RoamAbout Wireless Manager options.

1. Select **Tools > Options** in the Console menu bar. The [Options window](#) opens.
2. In the left-panel tree, expand the Console folder and select RoamAbout Wireless Manager. The right-panel RoamAbout Wireless Manager view is displayed.
3. Select the desired checkboxes to specify which right-panel tabs you want displayed in the RoamAbout Wireless Manager window.




## How to View AP Configuration Settings

---

Use the RoamAbout Wireless Manager right-panel tabs to view configuration settings for the AP3000 and AP4102 devices you have selected in the left-panel device tree. There are six right-panel tabs that display different AP configuration information.

Information on:

- [AP Interfaces Tab](#)
- [AP Interface Security Tab](#)
- [AP Clients Tab](#)
- [AP Neighbors Tab](#)
- [Neighbor Scan Settings Tab](#)
- [RADIUS Server Settings Tab](#)

The tabs provide a handy toolbar that lets you retrieve device information and quickly access some of RoamAbout Wireless Manager's features: 

**Retrieve** 

Retrieves current data for the devices selected in the left-panel device tree.

**Scan for Neighbors Now** 

In the Neighbor Scan Settings tab, click this button to perform a Neighbors scan for the device selected in the right-panel tab.

**Configure** 

Opens the Element Configuration window where you can [configure settings](#) for the device selected in the right-panel tab.

**Monitor** 

Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

RoamAbout Wireless Manager provides table options and tools that let you customize table properties, and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right-mouse click on a column heading or anywhere in the table body.


## Right-Click Menu Options



Right-click on a column heading or anywhere in the table body to see the following options:

- **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.
- **AP Statistics Monitor** - Lets you monitor 802.11 statistics for the active interfaces on the device selected in the right panel.
- **AP Error Statistics Monitor** - Lets you monitor 802.11 error statistics for the active interfaces on the device selected in the right panel.
- **Select All** - selects all of the entries in the table.
- **Table Tools**
  - **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.

## *AP Interfaces Tab*

This right-panel tab provides basic information for each AP interface and virtual interface on the AP3000 and AP4102 devices you have selected in the left-panel tree.

-  - Retrieves current data for the devices selected in the left-panel device tree.




-  - Opens the Element Configuration window where you can [configure settings](#) for the AP4102 device selected in the right-panel tab.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

The tab provides the following information for each interface:

- State - Enabled or Disabled
- IP Address
- MAC Address
- Type - 802.11 a or 802.11 b/g
- Description
- SSID
- VLAN ID
- Radio Channel
- Antenna Mode
- Antenna Mode Control
- Fixed Antenna Type

### *AP Interface Security Tab*

Use this right-panel tab to view security settings and authentication settings for each AP interface and virtual interface on the AP3000 and AP4102 devices you have selected in the left-panel tree. Select either the **Security Settings** or **Authentication Settings** button at the top of the tab.

-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Opens the Element Configuration window where you can [configure settings](#) for the AP4102 device selected in the right-panel tab.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.


The tab provides the following information for each interface:

- State - Enabled or Disabled
- IP Address

- MAC Address
- Type - 802.11 a or 802.11 b/g
- SSID
- Security Settings:
  - Auth type
  - Data Encrypt
  - WPA Clients
  - Multicast Cipher Mode
  - WPA Pre-Shared Key Type
- Authentication Settings:
  - 802.1X Mode
  - Broadcast Key Refresh Rate
  - Session Key Refresh Rate
  - 802.1X Session Timeout
  - MAC Authentication Type
  - MAC Authentication Session Timeout
  - Local MAC Authentication Default
- VLAN ID
- Radio Channel

### *AP Clients Tab*

This right-panel tab provides information on any wireless devices currently connected to the AP3000 and AP4102 devices you have selected in the left-panel tree.



-  - Retrieves current data for the devices selected in the left-panel device tree.

The tab provides the following information for each client device:

- AP IP Address
- AP Interface
- MAC Address (client)
- Association ID

- VLAN ID
- Authenticated
- Forwarding
- Associated
- Key Type
- Associated Time
- Last Authenticated Time
- Last Associated Time
- Last Disassociated Time



### *AP Neighbors Tab*

This right-panel tab lists the neighbors (other AP devices that are broadcasting network names) of the AP3000 and AP4102 devices you have selected in the left-panel tree. This list reflects the last data retrieved by a neighbor scan. To perform a new scan, click the scan button  in the Neighbor Scan Settings Tab, then come back to this tab and click Retrieve  to update the data. The following information is listed:



- Device IP Address (AP)
- Interface (AP)
- BSSID
- SSID
- Channel
- RSSI

### *Neighbor Scan Settings Tab*

Use this right-panel tab to view the settings configured for performing neighbor scans for each AP3000 and AP4102 device you have selected in the left-panel tree.

-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Performs an immediate Neighbor Scan for the selected devices, and stores the information on the devices. You can view the scan results in the

AP Neighbors tab. A scan is performed regardless of whether scanning is enabled or disabled on the device.


-  - Opens the Element Configuration window where you can [configure settings](#) for the AP4102 device selected in the right-panel tab.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.



The following scan settings are listed in this tab:

- IP Address
- RADIUS Authenticate - Whether RADIUS Authentication is enabled or disabled on the device.
- a Scanning - Whether scanning is enabled or disabled on the 802.11 a interface.
- a Radio Scan Interval - The AP Scan Interval (in minutes) for the 802.11 a interface.
- a Radio Scan Duration - The AP Scan Duration (in milliseconds) for the 802.11 a interface.
- b/g Scanning - Whether scanning is enabled or disabled on the 802.11 b/g interface.
- b/g Radio Scan Interval - The AP Scan Interval (in minutes) for the 802.11 b/g interface.
- b/g Radio Scan Duration - The AP Scan Duration (in milliseconds) for the 802.11 b/g interface.

### *RADIUS Server Setting Tab*

This right-panel tab lets you view the settings for communication between the selected AP3000 and AP4102 devices and a primary and secondary RADIUS server. It also displays whether RADIUS accounting is enabled for your SNMPv3 devices that support it. RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. For more information on accounting functionality, refer to your RADIUS server documentation.

-  - Retrieves current data for the devices selected in the left-panel device tree.

-  - Opens the Element Configuration window where you can [configure settings](#) for the AP4102 device selected in the right-panel tab.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

The following settings are listed for either the Primary or Secondary Server, depending on what button you have selected at the top of the tab:

- IP Address
- 802.1X Supplicant Enabled
- RADIUS Host
- Port - the UDP port number (1-65535) on the RADIUS server that the device will send authentication requests to.
- Timeout (seconds) - The amount of time in seconds the device will wait for the RADIUS server to respond to a request.
- Retransmit Attempts - The number of times the device will resend a request if the RADIUS server does not respond.
- Accounting - Whether RADIUS Accounting is enabled or disabled on the device.
- Accounting Port - The UDP port number (1-65535) on the RADIUS server that the device will send accounting requests to.
- Interim Update Timeout (seconds)

---

## Related Information

For information on related tasks:

- [How to Configure a Device](#)
- [How to Monitor AP Statistics](#)

## How to View R2 Configuration Settings

---

Use the RoamAbout Wireless Manager right-panel tabs to view configuration settings for the RoamAbout R2 devices you have selected in the left-panel device tree. There are four right-panel tabs that display different R2 configuration information.

Information on:

- [R2 Wireless Configuration Tab](#)
- [R2 Management Information Tab](#)
- [R2 Misc Controls Tab](#)
- [R2 Error Log Info Tab](#)

The tabs provide a handy toolbar that lets you retrieve device information and quickly access device statistics: 

**Retrieve** 

Retrieves current data for the devices selected in the left-panel device tree.

**Monitor** 

Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel.

RoamAbout Wireless Manager provides table options and tools that let you customize table properties, and find, filter, sort, print, and export information in a table. You can access these Table Tools through a right-mouse click on a column heading or anywhere in the table body.

### Right-Click Menu Options

Right-click on a column heading or anywhere in the table body to see the following options:



- **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.
- **AP Statistics Monitor** - Lets you monitor 802.11 statistics for the active interfaces on the device selected in the right panel.



- **AP Error Statistics Monitor** - - Lets you monitor 802.11 error statistics for the active interfaces on the device selected in the right panel.
- **Table Tools**
  - **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.

### *R2 Wireless Configuration Tab*

This tab provides basic information for each interface on the R2 devices selected in the left-panel tree.

-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.



The tab provides the following information for each interface:

- IP Address
- IF Description
- PC Card Type
- PC Card Versions
- Wireless Network Name
- PC Card MAC Addr
- Station Name
- Current Channel

- Bridge Mode
- AP Density
- Secure Access
- Multicast TX Rate
- IntraBSS Relay
- Reset Options

### *R2 Management Information Tab*

This tab provides information on management parameters for each device selected in the left-panel tree.



-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

The tab provides the following information for each device:

- IP Address
- Wired MAC Address
- Memory Size
- Power Ups
- Management Resets
- Unsolicited Management Resets
- Telnet
- WEB

### *R2 Misc Controls Tab*

This tab provides miscellaneous information for each device selected in the left-panel tree.



-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

The tab provides the following information for each device:

- IP Address
- Product Name
- Spanning Tree
- BOOTP
- DHCP
- Baud
- Password
- Save to NVRAM
- Reset

### *R2 Error Log Info Tab*

This tab provides error log information for the devices selected in the left-panel tree. The tab displays the actual error log table on the device.

-  - Retrieves current data for the devices selected in the left-panel device tree.
-  - Opens the AP Statistics Monitor window where you can [monitor 802.11 statistics](#) for the device selected in the right-panel tab.

The tab provides the following information for each device:

- IP Address
- Instance
- Index
- Time Stamp
- Reset Number
- Info

---

### **Related Information**

For information on related tasks:

- [How to Configure a Device](#)
- [How to Monitor AP Statistics](#)