



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

***Policy Manager 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® Policy Manager Help ..... 1
  - Policy Manager Overview ..... 1
  - Document Version ..... 1
- Policy Manager Configuration Considerations ..... 3**
  - General Considerations ..... 3
    - Authenticating without Policy ..... 3
    - Terminating Role Override Sessions ..... 4
    - Port-Level MAC to Role Mappings ..... 5
    - Import From Device ..... 5
    - Flood Control ..... 5
  - C1 Considerations ..... 5
    - Policy Support ..... 5
    - Rule Limits ..... 6
  - N-Series Considerations ..... 6
    - Role Precedence for the N-Series Platinum ..... 6
  - C2 and B2 Considerations ..... 7
  - C3 and B3 Considerations ..... 8
  - Mixed-Stack C2/C3 and B2/B3 Considerations ..... 9
  - 7100 Considerations ..... 10

---

ExtremeXOS Considerations .....	11
NAC Controller Configuration .....	12
NAC Controllers Require Separate Domains .....	12
Modifying NAC Controllers Preconfigured Policy .....	12
Modifying the Downstream Default Policy .....	12
Configuring LAG on NAC Controllers .....	13
Configuring LAG on Layer 3 NAC Controllers - Upstream Ports .....	13
Configuring LAG on Layer 3 NAC Controllers - Downstream Ports .....	13
Configuring LAG on Layer 2 NAC Controllers - Upstream Ports .....	13
Configuring LAG on Layer 2 NAC Controllers - Downstream Ports .....	14
ExtremeWireless Wireless Controller Configuration .....	14
Version Supported .....	14
Policy Rules .....	14
Supported Rule Types .....	15
"No Change" Filter Sets .....	15
Rule Actions .....	15
Rule Directions .....	16
Rule Limits .....	17
Role Default Actions .....	17
Class of Service .....	17
Rate Limits .....	17
Internal VLAN .....	18
Policy Inheritance .....	18
Configuring RADIUS Servers .....	19
Other Considerations .....	20
<b>Getting Started with Policy Manager .....</b>	<b>21</b>

---

Policy Manager Overview .....	21
Quick Tour .....	23
Understanding Policy Domains .....	24
Understanding Roles .....	25
Understanding Services .....	27
Working with Service Groups .....	28
Understanding Traffic Classification Rules .....	30
Adding Devices .....	30
Configuring Devices for Authentication .....	31
Working with Device Groups .....	32
Viewing Port Configuration Information .....	33
Working with Port Groups .....	34
Working with VLANs .....	35
Viewing Classes of Service .....	36
Using Policy Manager Wizards .....	37
Saving the Domain .....	38
Enforcing .....	39
Accessing Policy Manager Help .....	40
Where to Go from Here .....	41
<b>Configuring Authentication .....</b>	<b>44</b>
Authentication Configuration Guide .....	45
Preliminary Reading .....	47
Installing Policy Manager .....	47
Post-Installation Reading .....	48
Planning Your Policies (Roles and Services) .....	48
Identifying Roles .....	49

---

Defining Services .....	49
Planning for Port Mode .....	50
Configuring End Users .....	51
Configuring a Windows Workstation as a DHCP Client .....	51
Configuring a Linux Workstation as a DHCP Client .....	52
Browser Requirements for Web-Based Authentication .....	52
Installing and Configuring the RADIUS Server .....	52
Installing the RADIUS Server .....	53
Adding RADIUS Client Devices .....	54
Adding RADIUS Users .....	55
Adding Native (Local) Users .....	55
Adding Domain Users .....	56
Configuring RADIUS in Policy Manager .....	57
Downloading the Firmware .....	57
Adding Devices to Policy Manager .....	58
Configuring the Port Mode .....	58
Configuring Devices as RADIUS Clients .....	59
Configuring Authentication on Devices .....	60
Web-Based Authentication .....	61
802.1X Authentication .....	62
MAC Authentication .....	62
802.1X+MAC Authentication .....	63
CEP Authentication .....	63
Quarantine Authentication .....	64
Auto Tracking Authentication .....	64
Testing Authentication .....	65

---

Testing Web-Based Authentication .....	65
Preparation .....	66
Testing Active/Discard Mode .....	67
Testing Active/Default Role Mode .....	69
Testing 802.1X Authentication .....	70
Preparation .....	70
Testing Active/Discard Mode .....	72
Testing Active/Default Mode .....	73
How to Configure Auto Tracking Authentication .....	75
Enable Auto Tracking Authentication .....	75
Set Session Properties .....	76
Auto Tracking and Destination Role Mappings Compatibility .....	77
802.1X Authentication Configuration Supplement .....	79
EAP MD5-Challenge End User (Supplicant) Setup .....	79
Windows XP and Windows 2000 End User (Supplicant) Setup .....	79
How to Speed up MD5 Prompt on XP Client .....	80
Linux SecureSupplicant Setup .....	81
EAP-TLS Certificate Setup .....	81
Windows 2000 AS Certificate Server Configuration .....	81
Windows XP Client Certificate Setup .....	82
802.11 Wireless Setup .....	83
RoamAbout R2 802.1X Configuration .....	83
How to Configure Quarantine Authentication .....	87
Define the Quarantine Role .....	87
Create a Quarantine Rule .....	88
Enable Quarantine Authentication .....	88



---

Set Session Properties .....	89
Configuring a Windows Server 2008 for RADIUS Authentication .....	91
Configuring Network Policy Server (NPS) .....	92
Specifying RADIUS Port Numbers .....	92
Adding RADIUS Client Devices .....	92
Adding a New Remote Access Policy .....	93
Registering NPS .....	94
Stopping and Restarting NPS .....	95
Creating Users in Active Directory .....	95
Creating a User .....	95
Specifying User Permissions .....	95
Configuring Devices and Testing Authentication .....	96
Configuring a Windows Server 2000 or 2003 for RADIUS Authentication .....	97
Configuring Internet Authentication Service (IAS) .....	98
Specifying RADIUS Port Numbers .....	98
Adding RADIUS Client Devices .....	98
Adding a New Remote Access Policy .....	99
Registering the IAS .....	100
Stopping and Restarting the IAS .....	100
Creating Users in Active Directory .....	101
Creating a User .....	101
Specifying User Permissions .....	101
Configuring Devices and Testing Authentication .....	102
<b>Policy Manager Concepts .....</b>	<b>104</b>
Policy .....	105
Role .....	105

---

What is a Role .....	105
Default Role .....	105
Policy Domains .....	106
Service .....	108
Rule .....	109
What is a Rule .....	109
Disabling Rules .....	109
Conflict Checking .....	109
Authentication .....	110
Authentication Types .....	110
Web-based Authentication (PWA or Port Web Authentication) .....	110
802.1X Authentication .....	111
MAC Authentication .....	112
CEP Authentication .....	112
Quarantine Authentication .....	113
Auto Tracking .....	113
RADIUS Authentication .....	114
How Authentication Works .....	114
Port Authentication States .....	115
Port Mode .....	116
Configuring Authentication in Policy Manager .....	119
Packet Tagging .....	119
VLAN to Role Mapping .....	120
Dynamic Egress .....	121
Setting Domain GVRP Status .....	125
Policy VLAN Islands .....	126

---

MAC Locking .....	126
Traffic Mirroring .....	127
Device Groups .....	128
System-Created Device Groups .....	128
User-Defined Device Groups .....	128
Port Groups .....	129
Pre-Defined Port Groups .....	129
User-Defined Port Groups .....	130
Network Resource Groups .....	130
Network Resource Topologies .....	130
Verifying .....	131
Background Verify on Startup .....	132
Enforcing .....	132
Controlling Client Interactions with Locks .....	133
Packet Flow Diagram .....	136
Traffic Classification Rules .....	137
Traffic Descriptions .....	138
Actions .....	139
VLAN Membership (Access Control) .....	139
Priority (Class of Service) .....	139
Classification Types and their Parameters .....	140
Layer 2 -- Data Link Classification Types .....	140
Layer 3 -- Network Classification Types .....	142
Layer 4 -- Application Transport Classification Types .....	149
Layer 7 -- Application Classification Types .....	153
Examples of How Rules are Used .....	154

---

Traffic Containment .....	154
Traffic Filtering .....	155
Traffic Security .....	155
Traffic Prioritization .....	156
Classification Rules Precedence .....	157
Precedence Scenarios .....	159
Scenario 1 .....	159
Scenario 2 .....	160
<b>Getting Started with Class of Service .....</b>	<b>161</b>
Class of Service Overview .....	161
Implementing CoS .....	162
Configuring CoS .....	163
Rate Limits .....	163
Transmit Queues .....	164
Flood Control .....	166
Class of Service Example .....	167
Configure the Classes of Service .....	169
Create the VoIP Core Role .....	169
Create a VoIP Core Service .....	170
Create a Rule .....	170
Creating the VoIP Edge Role .....	170
Create a VoIP Edge Service .....	170
Create a Rule .....	170
Creating the H.323 Call Setup Role .....	170
Create a H.323 Call Setup Service .....	171
Create a Rule .....	171

---

Apply the Roles to Network Devices .....	171
How to Create a Class of Service .....	172
Creating a Class of Service .....	172
Creating Class of Service Port Groups .....	174
Deleting a Class of Service .....	175
How to Configure Transmit Queues .....	176
Transmit Queue Configuration .....	176
Transmit Queue Bandwidth Configuration .....	177
Strict Mode .....	177
Weighted Fair Mode .....	178
Enhanced Transmission Selection Mode .....	179
Low Latency Queuing .....	181
Setting the Arbiter Mode .....	181
Transmit Queue Rate Shapers .....	181
How to Configure Flood Control .....	183
How to Define Rate Limits .....	186
Defining Rate Limits .....	186
Removing a Rate Limit .....	187
Advanced Rate Limiting by Port Type .....	189
Configuring Rate Limit Mappings .....	190
Associating Rate Limits with a Class of Service .....	190
ToS/DSCP Value Definition Chart .....	192
Priority-Based Rate Limits .....	194
How to Define Priority-Based Rate Limits .....	196
Defining Priority-Based Rate Limits .....	196
Removing a Priority-Based Rate Limit .....	198

---

<b>How To Use Policy Manager</b> .....	<b>199</b>
How to Add and Delete Devices .....	200
Using Console to Discover Devices .....	200
Using Console to Import Devices .....	201
Adding a Single Device .....	201
Deleting Devices from the Database .....	202
Disabling Policy Support from an XOS Device .....	202
How to Add and Remove Device Groups .....	204
Adding a Device Group .....	205
Adding Devices to a Device Group .....	205
Using the Add Device Window .....	205
Using the Device Group Selection Window .....	205
Dragging and Dropping Devices .....	206
Removing Devices from a Device Group .....	206
Renaming a Device Group .....	207
Deleting a Device Group .....	207
How to Configure Anti-Spoofing .....	208
Anti-Spoofing Overview .....	208
DHCP Snooping .....	209
DHCP Snooping Port Types .....	210
DHCP MAC Verify .....	210
Dynamic ARP Inspection (DAI) .....	211
IP Source Guard .....	211
Duplicate IP Checking .....	211
Populating the MAC-to-IP Binding Table .....	212
Bindings Created by DHCP Snooping .....	212

---

Bindings Created by DAI or IP Source Guard .....	213
Expiration of Bindings .....	213
Implementing Anti-Spoofing in Your Network .....	213
Using DHCP Snooping Only .....	213
Using DAI, IP Source Guard, and Duplicate IP Detection .....	214
Anti-Spoofing Configuration .....	215
Port Classes .....	215
Managing the Binding Table .....	216
Anti-Spoofing Configuration Steps .....	216
Configure Port Classes .....	216
Configure Ports .....	217
Configure Devices .....	218
Configuration Example .....	218
How to Configure CEP .....	220
How to Configure Devices .....	223
Using the Device Configuration Wizard .....	223
Select Options to Configure .....	224
Authentication Tab .....	224
RADIUS Tab .....	224
General Tab .....	225
Configure Settings .....	226
If you have selected to configure Authentication .....	226
Authentication Configuration Window .....	226
General Authentication Settings Window .....	227
Global Timeout Settings Window .....	228
Enhanced Login Mode Window (web-based authentication only) .....	229

---

Web Authentication URL Window (web-based authentication only) .....	229
Web Authentication IP Address Window (web-based authentication only) .....	229
Login Web Page Banner Window (web-based authentication only) .....	229
Web Authentication Logo Display Status Window (web-based authentication only) .....	230
DNS Server Configuration Window (web-based authentication only) .....	230
Guest Networking Window (web-based authentication only) .....	230
Redirect Time Window (web-based authentication only) .....	231
MAC Mask Window .....	231
MAC User Password Window .....	232
CEP Role Mapping Window .....	232
CEP Detection Window .....	232
If you have selected to configure RADIUS .....	232
RADIUS Authentication Server(s) Window .....	232
RADIUS Accounting Server(s) Window .....	232
RADIUS Authentication Client Settings Window .....	233
RADIUS Accounting Client Settings Window .....	233
Application Shared Secret Window .....	234
RADIUS Response Mode Window .....	234
If you have selected General .....	235
MAC Locking Window .....	235
Device Level Role (C1 Only) Window .....	235
Rule Accounting Window .....	235
Class of Service Mode Window .....	236



---

Invalid Role Action Window .....	237
RFC3580 VLAN Authorization Status Window .....	237
Select Devices .....	237
Using the Device Tabs .....	237
How to Configure Ports .....	239
Using the Port Configuration Wizard .....	239
Select Options to Configure .....	240
Configure Settings .....	241
Port Authentication Configuration Window .....	241
Port Mode Window (802.1X, MAC, Web-Based, CEP, Quarantine, Auto Tracking) .....	242
Hold Time Window (802.1X, MAC, Web-Based) .....	243
Authentication Request Period Window (802.1X) .....	243
User Timeout Window (802.1X) .....	243
Authentication Server Timeout Window (802.1X) .....	243
Port Handshake Requests Window (802.1X) .....	243
Automatic Re-Authentication Window (802.1X, MAC) .....	244
Authenticated User Counts Window (802.1X, MAC, Web-Based) ...	244
Timeout Number Window (Web-Based) .....	244
CEP Protocol Enable Window .....	244
Default Role Window .....	244
Drop VLAN Tagged Frames Window .....	245
Frozen Status Window .....	245
MAC Locking Window .....	245
TCI Overwrite Window .....	245
Disable Traffic Classification Types Window .....	246

---

Egress Policy Status Window .....	246
RFC3580 VLAN Authorization Window .....	246
Tagged Packet VLAN to Role Mapping Window .....	247
MAC/IP to Role Mapping Window .....	247
Select Ports .....	248
Using the Port Properties Window .....	248
Assigning Default Roles to Ports .....	249
Single Port .....	249
Multiple Ports .....	249
Clearing Default Roles from Ports .....	250
Single Port .....	250
Multiple Ports .....	250
Disabling Traffic Classification Rules on Ports .....	251
Enabling CEP Protocol .....	251
Enabling Drop VLAN Tagged Frames .....	251
Freezing/Unfreezing Ports .....	252
Locking MAC Addresses to Ports .....	252
Setting Port Authentication .....	252
Terminating a Session .....	252
Single Port .....	253
Multiple Ports .....	254
How to Create a Network Resource .....	255
How to Create a Port Group .....	258
Creating a Port Group .....	258
Adding Ports to a Port Group .....	258
Removing Ports from a Port Group .....	259

---

How to Create a Quarantine Role .....	260
Modifying the Quarantine Role .....	261
Modifying Default Values .....	261
Adding/Removing Services .....	261
Setting the Quarantine Role as the Default Role on a Port .....	262
How to Create a Role .....	263
Using the Role Wizard .....	263
Using the Role Tabs .....	266
Modifying a Role .....	267
Adding Services to Roles .....	267
Removing Services from a Role .....	268
Modifying a Role's Default Class of Service .....	269
Modifying a Role's Default Access Control .....	269
Modifying a Role's Description .....	269
Modifying a Role's Ports .....	269
Deleting a Role .....	270
How to Create a Service .....	272
Using the Service Wizard .....	273
Using the Service Tabs .....	281
Creating an Automated Service .....	281
Creating a Manual Service .....	282
Modifying a Service .....	283
Modifying a Service Description .....	283
Modifying a Service Name .....	283
Modifying the Roles for a Service .....	283
Modifying the Rules for a Manual Service .....	284

---

Modifying an Automated Service .....	284
Saving Services to a .pmd File .....	285
Deleting a Service .....	286
How to Create a Service Group .....	288
Creating a Service Group .....	288
Adding Services to a Service Group .....	288
Removing Services from a Service Group .....	289
How to Create a VLAN .....	290
Creating a VLAN .....	291
Editing an Island VLAN ID .....	291
Deleting a VLAN .....	291
Turning Off Getting VLANs on Startup .....	292
How to Create a Policy VLAN Island .....	293
Creating a VLAN Island .....	293
Modifying a VLAN Island .....	293
Deleting a VLAN Island .....	294
How to Create and Use Domains .....	295
Creating a New Domain .....	296
Opening a Domain .....	296
Assigning Devices to a Domain .....	296
Removing Devices From a Domain .....	297
Importing a File into a Domain .....	298
Exporting a Domain to a File .....	298
Generating a Policy Report for a Domain .....	299
Importing Data from a Domain .....	299
Saving a Domain .....	300

---

Reading a Domain .....	300
Renaming a Domain .....	301
Deleting a Domain .....	301
How to Create or Modify a Rule .....	302
Using the Classification Rule Wizard .....	303
Using the Rule General Tab .....	306
Disabling/Enabling a Rule .....	307
Deleting a Rule .....	308
How to Define Traffic Descriptions .....	309
How to Define Well-Known IDs .....	311
How to Enable Passive Domain Mode .....	313
How to Filter, Find, and Sort .....	315
Filtering .....	315
Finding .....	316
Sorting .....	316
How to Freeze/Unfreeze a Port .....	318
Freezing/Unfreezing a Port .....	318
Freezing/Unfreezing a Device .....	319
How to Import From Device .....	320
Using the Import From Device Wizard .....	320
Import From Device .....	320
Device Selection .....	321
Read From Device .....	321
Organize and Update .....	324
Merge Rules .....	324
How to Initialize the Policy Manager Database .....	326

---

How to Lock MAC Addresses to Ports .....	327
Dynamic MAC Locking .....	327
Static MAC Locking .....	328
On a Single Port .....	328
On Multiple Ports .....	329
Rule Accounting and Rule Hit Reporting .....	331
Configuring Rule Accounting and Reporting .....	331
Viewing Rule Usage Information .....	333
Viewing Policy Rule Hit Reporting .....	334
How to Select on Add/Remove Windows .....	337
Selecting single items .....	337
Selecting multiple sequential items .....	337
Selecting multiple non-sequential items .....	338
How to Set Policy Manager Options .....	339
Default Class of Service .....	339
Dialog Boxes .....	340
Optional Views .....	341
Name Resolution (PM) .....	341
Policy Rule Hit Reporting .....	341
Ports .....	343
Startup .....	343
SNMP Options .....	344
Tab Configuration .....	345
Welcome View .....	346
Wireshark .....	347
How to Use Wireshark® to Analyze a Role's Behavior .....	348

---

Launching Wireshark .....	349
Launching Against a Data Capture .....	349
Launching Against Live Local Traffic .....	350
Launching Against Live Remote Traffic .....	352
Viewing Wireshark .....	353
Wireshark Color Filter Scheme .....	353
Determining Rule Hit .....	356
Viewing Color Filters .....	357
Policy Classification Rules Window .....	359
Rules for the Current Domain .....	359
Rules for All Domains .....	362
<b>Policy Manager Right-Panel Tabs .....</b>	<b>365</b>
Anti-Spoofing Tab (Device) .....	366
Device Configuration .....	366
General Settings .....	367
Violation Actions .....	368
Port Configuration .....	370
Station Bindings .....	371
Arbiter Mode Tab (Transmit Queue Port Group) .....	374
Slice Configuration .....	376
Slice Distribution .....	376
Authentication Tab (Device) .....	377
General Settings .....	378
RFC3580 VLAN Authorization .....	380
Global Authentication Settings Tab .....	380
Web Authentication Settings Tab .....	381

---

General Tab .....	381
Guest Networking Tab .....	383
Web Login Tab .....	384
DNS Tab .....	386
MAC Authentication Settings Tab .....	386
CEP Tab .....	387
CEP Role Mappings Tab .....	388
CEP Detection Tab .....	389
Authentication Tab (Device Group/Island) .....	392
Authentication Tab (My Network/All Devices Folder) .....	395
CoS - Rate Limit Mappings Tab (Rate Limit) .....	398
CoS - Rate Limit Mappings Tab (Rate Limit Port Group) .....	400
CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group) .....	402
Flood Control Rate Limits Tab (Flood Control Port Groups) .....	405
Details View Tabs .....	408
Details View Tab (802.1p Priorities Folder) .....	409
Details View Tab (Rate Limits Folder) .....	411
Details View Tab (CoS Components Folder) .....	413
Details View Tab (Device) .....	414
Details View Tab (Device Group) .....	417
Details View Tab (My Network/All Devices Folder) .....	419
Details View Tab (Network Resources Folder) .....	421
Details View Tab (Network Resource Topologies Folder) .....	423
Details View Tab (Network Resource Topology) .....	425
Details View Tab (Roles Folder) .....	427
Details View Tab (Service) .....	429



---

Details View Tab (Services Folder) .....	433
Details View Tab (Service Group) .....	435
Details View Tab (Service Groups Folder) .....	437
Details View Tab (User-Defined Port Groups Folder) .....	438
Details View Tab (VLANs Folder) .....	439
Device Support Tab (Role) .....	441
Devices Area .....	442
Classification Rules Area .....	442
Excluded Table/Included Table .....	443
Unmatched Frames .....	443
Device Support Tab (Rule) .....	445
Device Support Tab (Service) .....	447
Top Panel .....	448
Classification Rules Area .....	448
General Tabs .....	450
General Tab (802.1p Priority) .....	451
Priority-Based Rate Limits .....	452
Usage .....	452
General Tab (Class of Service) .....	454
General .....	455
Rate Limiting/Rate Shaping .....	457
Index Numbers .....	457
General Tab (Device) .....	460
General .....	460
Profiles .....	461
Class of Service Mode .....	461

---

General Tab (Network Resource Group) .....	464
General Tab (Rate Limit) .....	466
Role-Based Configuration Tab .....	468
Priority-Based Configuration Tab .....	469
General Tab (Role) .....	471
Default Actions .....	473
Services .....	474
General Tab (Roles Folder) .....	476
General Tab (Rule) .....	477
General Area .....	477
Traffic Description Area .....	479
Actions Area .....	479
General Tab (Service) .....	483
Traffic Description Area .....	484
Actions Area .....	484
General Tab (Transmit Queue) .....	488
Enable Rate Shaping .....	488
Low Latency Queue Status .....	489
General Tab (VLAN) .....	490
General .....	490
Tagged Packet VLAN to Role Mapping .....	491
Authentication-Based VLAN to Role Mapping .....	492
Island Topology Tab (Policy VLAN Islands) .....	494
(Island) - VIDs Tab .....	494
(Island) - Devices Tab .....	496
MAC Locking Tab (Device) .....	498

---

Locked MAC Addresses .....	499
MAC Locking Tab (Device Group/Island) .....	501
Static MACs .....	501
Locked MAC Addresses .....	502
MAC Locking Tab (My Network/All Devices Folder) .....	504
Static MACs .....	504
Locked MAC Addresses .....	505
MAC Locking Tab (Port Group) .....	506
Static MACs .....	506
Locked MAC Addresses .....	507
Mappings Tab (Role) .....	509
MAC to Role Mapping .....	510
IP to Role Mapping .....	511
Tagged Packet VLAN to Role Mapping .....	511
Authentication-Based VLAN to Role Mapping .....	513
Ports Tab (Device) .....	514
Ports Tab (Port Group) .....	517
Ports Tab (Rate Limit Port Group) .....	520
Ports Tab (Role) .....	525
Ports Tab (Transmit Queue Port Group) .....	530
Ports Tab (Flood Control Port Groups) .....	535
Port Usage Tab (Device) .....	538
End User Sessions Tab .....	538
Rate Limit Violations Tab .....	544
CEP Usage Tab .....	545
Port Usage Tab (Device Group/Island) .....	547

---

End User Sessions Tab .....	547
Rate Limit Violations Tab .....	553
CEP Usage Tab .....	554
Port Usage Tab (My Network/All Devices Folder) .....	556
End User Sessions Tab .....	556
Rate Limit Violations Tab .....	562
CEP Usage Tab .....	563
Port Usage Tab (Port Group) .....	565
End User Sessions Tab .....	565
Rate Limit Violations Tab .....	571
CEP Usage Tab .....	572
Precedence Tab (Rate Limits Folder) .....	574
RADIUS Tab (Device) .....	576
Authentication Tab .....	577
RADIUS Authentication Client Settings .....	577
Application Shared Secret (Legacy) .....	579
Authentication RADIUS Server(s) Table .....	580
Accounting Tab .....	582
RADIUS Accounting Client Settings .....	583
Accounting RADIUS Servers Table .....	584
Port Configuration Tab .....	586
RADIUS Tab (Device Group/Island) .....	588
RADIUS Tab (My Network/All Devices Folder) .....	591
Role/Rule Tab (Device) .....	594
Invalid Role Action .....	594
Device Level Role (C1 Devices Only) .....	595

---

Rule Accounting / Rule Hit Reporting .....	595
Disabled Ports (Rule / Rate Limit Hit) .....	597
Rule Usage Tab .....	598
Rule Usage Tab (Rule) .....	600
Summary Tab (Rate Limit Port Groups Folder) .....	602
Summary Tab (Transmit Queue Port Groups Folder) .....	604
Summary Tab (Flood Control Port Groups) .....	606
VLAN Egress Tab (Role) .....	608
VLANs Tab (Policy VLAN Islands) .....	610
(VLAN) - VIDs Tab .....	610
(VLAN) - Role Mappings Tab .....	612
<b>Policy Manager Windows .....</b>	<b>614</b>
Add/Edit CEP Detection Rule Window .....	615
CEP Detection Settings .....	616
Add Device Window .....	618
Add/Edit CoS to Rate Limit Mappings Window .....	620
Add RADIUS Accounting Server Window .....	622
Add RADIUS Authentication Server Window .....	625
Add/Remove Devices Window (VLAN Islands) .....	628
Add/Remove Mappings Window (Port-Level Mappings) .....	630
Add/Remove Network Elements Window .....	632
Add/Remove Ports Window (Rate Limit and Transmit Queue Port Groups) .....	634
Add/Remove Ports Window (Rule Usage Auto Clear) .....	636
Add/Remove Ports Window (User-Defined Port Groups) .....	638
Add/Remove Services Window (Roles) .....	640

---

Add/Remove Services Window (Service Groups) .....	643
Add Static MAC Window .....	645
Assign Devices to Domain Window .....	648
Class of Service Configuration Window .....	652
Classes of Service Usage Window .....	656
CoS Rate Limit Violations Window .....	658
Create Class of Service Window .....	660
General .....	660
Rate Limit Configuration .....	662
Create Classification Rule Window .....	663
Create Mixed-Stack C2/C3 Domain Tool .....	665
"Show" Radio Buttons .....	666
Left Panel .....	666
Right Panel .....	667
Create Rate Limit/Shaper Window .....	670
Create VLAN Window .....	672
Device Configuration Wizard Add RADIUS Accounting Server Window .....	674
Device Configuration Wizard Add RADIUS Authentication Server Window .....	677
Device Group Selection Window .....	681
Domain Tab Configuration Window .....	682
Edit Actions Window .....	684
Edit Bandwidth Configuration Window .....	685
Strict .....	685
Weighted Fair Queuing .....	686
Enhanced Transmission Selection .....	687

---

Use Per-Port Type Arbiter Mode .....	689
Slice Configuration .....	689
Slice Distribution .....	689
Edit RADIUS Accounting Server Window .....	691
Edit RADIUS Authentication Server Window .....	693
Edit Rate Limit/Shaper Window .....	695
Edit Rule Window .....	697
Layer Area .....	698
Type Area .....	698
Value Area .....	699
Enforce Preview Window .....	700
"Show" Radio Buttons .....	701
Left Panel .....	701
Right Panel .....	702
Event Details Window .....	707
Event Log .....	709
Right-Click Menu Options .....	710
Filter Window .....	711
Find Window .....	713
Import from Domain Window .....	715
Data Elements to Import .....	715
Application of Imported Data Elements .....	718
Import from File Window .....	721
Data Elements to Import .....	721
Global Domain Data .....	724
Application of Imported Data Elements .....	725

---

Main Window .....	727
Dialog Boxes (Messages) .....	728
Icons .....	728
Status Bar Icons .....	729
Left Panel .....	731
Roles/Services Tab .....	732
Roles Tree .....	732
Service Repository Tree .....	732
Network Elements/Port Groups Tab .....	734
My Network Tree .....	734
Port Groups Tree .....	736
Access Control Configuration .....	737
Class of Service Configuration .....	738
Network Resources Configuration .....	739
Policy Manager Menus .....	742
File Menu .....	742
Edit Menu .....	744
View Menu .....	746
Tools Menu .....	747
Domain Menu .....	751
Applications Menu .....	753
Help Menu .....	753
Right-click Menu Options .....	754
Right Panel .....	755
Status Bar .....	756
Toolbar .....	757



---

Policy Manager Options Window .....	760
Default Class of Service .....	760
Dialog Boxes .....	762
Name Resolution (PM) .....	762
Optional Views .....	763
Policy Rule Hit Reporting .....	764
Ports .....	766
Startup .....	767
SNMP Options .....	768
Tab Configuration .....	769
Welcome View .....	771
Wireshark .....	772
Port Properties Anti-Spoofing Tab .....	774
Configuration Tab .....	774
Station Bindings Tab .....	776
Port Properties Authentication Configuration Tab .....	779
General Tab .....	779
Port Mode .....	780
RFC3580 VLAN Authorization Tab .....	782
Login Settings Tab .....	784
Automatic Re-Authentication Tab .....	786
Authenticated User Counts Tab .....	786
CEP Access Tab .....	788
Port Properties General Tab .....	790
General Tab .....	790
General .....	791

---

Role Config .....	793
Mappings Tab .....	794
MAC/IP to Role Mapping .....	795
Tagged Packet VLAN to Role Mapping .....	795
Drop VLAN Tagged Frames Tab .....	796
Disabled Traffic Classification Types Tab .....	797
Port Properties MAC Locking Tab .....	799
General Tab .....	799
MAC Locking Limits .....	800
Static MACs .....	801
Locked MAC Addresses Tab .....	801
Port Properties Port Usage Tab .....	803
End User Sessions Tab .....	803
End User Session Settings Tab .....	809
Rate Limit Violations Tab .....	812
CEP Usage Tab .....	814
Port Properties Rule Usage Tab .....	816
Pre-Defined Well-Known IDs Window .....	818
Port Tab .....	818
IP Protocol Tab .....	820
Role/Service Usage Window .....	822
Selection View (Egress VLANs) .....	824
Selection View (Roles) .....	826
Selection View (VLANs) .....	828
Set Authentication Port Mode to Inactive/Default Role Window .....	830
Slice Percentages Window .....	832

---

Slice Configuration .....	832
Sort Window .....	834
ToS/DSCP Configuration Window .....	836
IP Type of Service Classification .....	836
ToS/DSCP Rewrite .....	836
Traffic Classification Type Wizard .....	839
Traffic Classification Layer .....	839
Traffic Classification Type .....	840

# Extreme Management Center® Policy Manager Help

---

Policy Manager enables the creation and deployment of role-based policies that dynamically control user access, network security, application prioritization and other parameters. Policy management and role-based administration are keys to effectively enforcing business and IT rules in the network infrastructure.

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

## Policy Manager Overview

Policy Manager simplifies the configuration of policies on networks, and deploys the policies on multiple devices throughout the switch fabric.

With Policy Manager, you can create policy profiles, called roles, that are assigned to the ports in your network. These roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. When authentication is enabled, users identify themselves to the network and are given customized access capabilities based on what role they serve in the organization.

Using the Policy Manager wizards and configuration tools, you can create multiple roles tailored to your specific needs, and set a default role for all or some of your network devices and ports. Basic Policy Manager operations include creating, editing, and deleting roles. You can also view role configuration on a per device and per port basis. In addition, Policy Manager allows you to verify that the roles enforced on your network device match the roles currently configured in the application. Policy Manager supports a maximum of 1,000 devices (25,000 ports) and 50 roles per policy domain, and can process a maximum of 250 classification rules with a maximum of 50 classification rules per role.

## Document Version

The following table displays the revision history for the Policy Manager Help documentation.

---

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

PN: 9034988-01

# Policy Manager Configuration Considerations

---

Review the following configuration considerations when installing and configuring NetSight Policy Manager.

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

## General Considerations

### Authenticating without Policy

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

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

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

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

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

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

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

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

## Terminating Role Override Sessions

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

## Port-Level MAC to Role Mappings

Enforcing port-level MAC to Role mappings could potentially remove rules that were created by NetSight Automated Security Manager (ASM) as an intrusion detection response.

## Import From Device

If you perform a Verify operation following an Import Policy Configuration from Device, the Verify may fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration.

Also, if you import from more than one device and the configuration is not the same on each device, Verify will fail. This is because the imported configuration will not match the configuration on any one device.

## Flood Control

Individual Class of Service granularity is unsupported on fixed switches, so if any CoS is assigned a Flood Control rate, all Class of Service on these devices will use that rate.

## C1 Considerations

Review the following considerations prior to configuring policy on C1 devices:

### Policy Support

Policy support on C1 devices utilizes both a port-level role and a device-level role. In Policy Manager, a role is a set of network access services made up of traffic classification rules. It may also contain default Access Control (VLAN) and/or Class of Service settings that will be applied to traffic not handled specifically by the rules contained in the role. Although both the device-level and port-level roles may contain all of these components, only certain portions of each role are used when applied to a port on a C1 device.

On the C1, classification rules are implemented at the device level through a device-level role. Policy Manager allows you to set a unique device-level role for each C1 device. The device-level role is a regular role that defines how inbound traffic is handled in terms of classification rules and default Class of Service



assignment. In other words, all classification rules are taken from the device-level role, and any rules defined in the port-level role are ignored when applied to a port. The Class of Service setting is also implemented through the device-level role and ignored in the port-level role. However, the default Access Control setting of the device-level role is ignored, and is defined through the port-level role.

Classification rules from the device-level role are only applied to ports which also have a port-level role applied (either statically or dynamically). This allows you to exclude the device-level role from uplink ports and hosts ports, by not applying a port-level role to these ports and not enabling authentication on them.

When a port-level role is applied to a port, it overrides any PVID and Class of Service settings defined on the port through Console or local management. When a device-level role is applied to a port, it also overrides these PVID and Class of Service settings, and overrides any Class of Service setting defined in the port-level role. It does **not** override any default Access Control setting defined in the port-level role.

In addition, if the port-level role's default Access Control is configured to deny traffic, then **all** inbound traffic will be discarded even if it matches a (forward) classification rule.

## Rule Limits

C1 devices limit the number of rules you can create for some classification types. Refer to the C1 information in the NetSight Release Notes to see which classification types limit the number of rules.

## N-Series Considerations

Review the following considerations prior to configuring policy on N-Series devices:

### Role Precedence for the N-Series Platinum

The following precedence determines the role (policy) that is being applied on a user/port on a N-Series Platinum device. The precedence used depends on whether the device is configured for multi-user authentication or single user authentication.

**Multi-User Authentication:**

Devices configured with multi-user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

- MAC override policy (created by ASM)
- Authenticated role
- MAC-to-Role mapping
- IP override policy (created by ASM)
- IP-to-Role mapping
- VLAN-to-Role mapping
- Default port role

**Single User Authentication:**

Devices configured with single user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

- MAC override policy (created by ASM)
- MAC-to-Role mapping
- IP override policy (created by ASM)
- IP-to-Role mapping
- Authenticated role
- VLAN-to-Role mapping
- Default port role

## C2 and B2 Considerations

Review the following considerations prior to configuring policy on C2 and B2 devices.

- When TCI Overwrite is enabled on a role, C2 and B2 devices support rewriting the 802.1p bit (CoS values) but not the 802.1Q bit (VLAN ID).
- On C2 and B2 gigabit and 10/100 ports, the number of rules per port is restricted. Refer to your C2 and B2 firmware release notes for the maximum number of rules that can be utilized on a port.
- C2 and B2 10/100 ports support two priority-based rate limits (inbound only). When creating a rate limit to be used on C2 and B2 10/100 ports, create the limit with either Low priority to associate the rate limit with priorities 0-3 or High priority to associate the rate limit with priorities 4-7. You can specify both Low and High priorities if you want to associate the rate limit with priorities 0-7.
- C2 and B2 devices do not support setting a default role on a logical port.

- On C2 and B2 devices, it is strongly recommended that you do not enforce rules that assign a Class of Service (CoS) that includes Priority 7. Doing so will interfere with stack communication.
- C2 and B2 devices do not allow a mask for an IP type of service (ToS) rewrite value associated with a class of service (CoS); they will always use ff.
- C2 and B2 devices do not support VLAN ID traffic classification rules. C2 devices (firmware 3.02.xx and newer) and B2 devices (firmware 2.xx.xx) support device-level VLAN to Role mapping. However, VLAN ID traffic classification rules can be configured on C2 devices with firmware versions 3.01.xx or older, using CLI.
- In order for VLAN to Role mapping to work on C2 and B2 devices, the device-level Authentication Type must be set to Multi-User (via the Device Configuration Wizard or the device [Authentication tab](#)) and the port-level "Number of Users Allowed" setting must be set to 2 (via the Port Configuration Wizard or the [Port Properties Authentication Configuration tab, Authenticated User Counts subtab](#)). (NOTE: This information applies to all EOS stackable devices.)
- B2 only. Each port on a policy-enabled B2 switch can support up to 100 rules and up to 10 masks. The maximum number of unique rules in a single switch or B2 stack is 100, while the maximum number of unique masks is 18. These unique rules and masks may be shared across any and all ports in a stack or switch.

## C3 and B3 Considerations

Review the following considerations prior to configuring policy on C3 and B3 devices.

- B3/C3 devices do not support TCI Overwrite. The B3/C3 will not overwrite 802.1Q VLAN bits, but will overwrite the 802.1p Priority bits.
- B3/C3 devices do not support Layer 3 ICMP rules.
- B3/C3 devices support role-based rate limiting. However, on the B3/C3, class of service inbound rate limiting works only on policy roles, not on policy rules.
- C3G and B3 devices have the following additional limitations:
  - Maximum 100 rules per policy role.
  - A system limitation of 768 unique rules.

- Maximum of 15 roles.
- C3 and B3 devices do not support setting a default role on a logical port.
- In order for VLAN to Role mapping to work on C3 and B3 devices, the device-level Authentication Type must be set to Multi-User (via the Device Configuration Wizard or the device [Authentication tab](#)) and the port-level "Number of Users Allowed" setting must be set to 2 (via the Port Configuration Wizard or the [Port Properties Authentication Configuration tab, Authenticated User Counts subtab](#)).

## Mixed-Stack C2/C3 and B2/B3 Considerations

Review the following considerations prior to configuring policy on mixed stacks of C2/C3 and B2/B3 devices. In addition, refer to the help topic on the [Create Mixed-Stack C2/C3 Domain Tool](#) for information on managing mixed stacks.

**NOTE:** While you can create mixed stacks of C2/C3 devices and mixed stacks of B2/B3 devices, you should not create mixed stacks of C and B devices (e.g. mixed stacks of C2/B2 or C3/B3 devices).

- It is strongly recommended that a C3 device be configured as the master in a mixed C2/C3 stack.
- It is strongly recommended that a B3 device be configured as the master in a mixed B2/B3 stack.
- When you have a mixed stack, all devices in the stack have the rule type and Class of Service limitations of a C3 or B3 device, despite the fact that the stack may report itself as a C2 or a B2. The device type that the stack reports is based on what switch is set as the master.
- Mixed stacks with a B3/C3 master support role-based rate limiting, however, class of service inbound rate limiting works only on policy roles, not on policy rules.
- A mixed stack containing a C2H or a B2 has the following limitations:
  - A single role limitation of 100 rules and 10 masks.
  - A system limitation of 100 unique rules and 18 unique masks.
  - No support for Layer 2 rules or Layer 3 ICMP type rules.
  - Maximum of 15 roles.
  - No support for rate limiting.

- A mixed stack containing a C2G has the following limitations:
  - A single role limitation of 100 rules and 10 masks.
  - A system limitation of 768 unique rules.
  - No support for Layer 2 rules.
  - Maximum of 15 roles.
  - No support for rate limiting.
- When adding a new device to a mixed stack, the ports should not go active unless the stack supports the policy configuration. Once a device has joined the stack, no roles should be enforced that are not supported on all devices. For example:

A C2K is added to an existing C3 stack.

  - If the number of masks in the C3 stack's current configuration exceed those allowed by the C2K, its ports cannot go active.
  - Once the C2K joins the stack, no roles can be enforced that exceed the limitations of any device.

## 7100 Considerations

- 7100 devices only support fixed IRL index reference mappings for the static CoS. The IRL Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed TXQ index reference mappings for the static CoS. The TXQ Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed COS - transmit queue mappings. The transmit queue specified for a Class of Service must match the 802.1p priority, or enforce will fail.
- TCI Overwrite configuration is not supported on the 7100. It is always enabled, and cannot be turned on or off using Policy Manager.

**NOTE:** [CoS components](#) can be managed at the device level to override settings enabled at the domain level.

## ExtremeXOS Considerations

- ExtremeXOS devices only support fixed IRL index reference mappings for the static CoS. The IRL Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce fails.
- ExtremeXOS devices only support fixed TXQ index reference mappings for the static CoS. The TXQ Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- ExtremeXOS devices only support fixed COS - transmit queue mappings. The transmit queue specified for a Class of Service must match the 802.1p priority, or enforce will fail.
- In order to configure port authentication when using Policy Manager, the port must be a member of a virtual router (VR).
- Low latency queue (LLQ)-enabled ports on ExtremeXOS devices can not be configured using Policy Manager, but must be set externally. For LLQ-enabled ports to function properly in Policy Manager, slices for LLQ-enabled queues must be 0.

**NOTE:** LLQ queues on ExtremeXOS devices in Policy Manager appear disabled.

- When stacking mode is enabled on ExtremeXOS devices, Transmit Queue 6 is reserved for stacking protocol traffic and can not have a rate limiter assigned or enforce fails.
- Policy Manager supports the use of VLANs on ExtremeXOS devices using policy functionality with the following exceptions:
  - VLANs cannot have a name containing "SYS\_VLAN". VLAN names containing "SYS\_VLAN" are automatically changed to the VLAN ID (VID).
  - VLAN names can only contain alphanumeric characters, dashes "-", and underscores "\_". All spaces and other non-alphanumeric used in VLAN names are automatically changed to an underscore "\_".
- ExtremeXOS devices support the first six bits of the Type of Service (ToS) value; additional bits are truncated.

**NOTE:** If Policy Manager truncates ToS bits on ExtremeXOS devices, the Information column on the Class of Service tab displays the message "Summit devices only support the top 6 bits of the TOS, so values may differ".

## NAC Controller Configuration

Review the following considerations prior to configuring policy on NAC Controller devices.

### NAC Controllers Require Separate Domains

NAC Controllers must be assigned to their own unique policy domain and cannot be combined with other switch types in a domain.

### Modifying NAC Controllers Preconfigured Policy

NAC Controllers are shipped with a default policy configuration already configured on the device. To modify this default policy configuration, you must create a domain for the NAC Controller, assign the NAC Controller to the domain, then import the policy configuration from the device into Policy Manager (File > Import > Policy Configuration from Device). You can then alter the policy configuration to define the authorization levels for the NAC process, as appropriate for your environment. If assessment will be enabled in the Extreme Networks NAC solution, you must add classifications rules to the Quarantine and Assessing policies to allow traffic to be forwarded to the assessment servers deployed on the network. When you have finished modifying the policy configuration, you must enforce it back to the NAC Controller.

---

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

---

### Modifying the Downstream Default Policy

Depending on the network configuration or circumstances, it's possible that traffic from the upstream side could be rerouted to the NAC Controller where it would be authenticated using the upstream source IP address. To avoid this problem, add a Layer 3 IP Address Source rule to the downstream default policy

configured on the NAC Controller, using the upstream IP subnets (or critical servers located in the upstream) and containing the traffic to a VLAN.

## Configuring LAG on NAC Controllers

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

### *Configuring LAG on Layer 3 NAC Controllers - Upstream Ports*

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

### *Configuring LAG on Layer 3 NAC Controllers - Downstream Ports*

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

### *Configuring LAG on Layer 2 NAC Controllers - Upstream Ports*

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



## *Configuring LAG on Layer 2 NAC Controllers - Downstream Ports*

1. Configure LAG on the NAC Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In Policy Manager options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use Policy Manager to assign the appropriate downstream role as the default role on the port. For instructions, see [Assigning Default Roles to Ports](#).
4. Select the port in the Device Details Tab, right-click and select Properties to open the Port Properties window.
  - a. Select the [Authentication Configuration tab](#) and the General subtab. Set the port mode Authentication Behavior to Active, and the Unauthenticated Behavior to Default Role. Uncheck "Disable 802.1X Authentication for this port," "Disable Web-Based Authentication for this port," and "Disable MAC Authentication for this port" and then Apply.
  - b. Select the [Authentication Configuration tab](#) and the Login Settings subtab. Set the Hold Time value to 120 seconds and then Apply.
5. Use the CLI to set the following command: `nodealias maxentries 4096 <lag port>`.

## **ExtremeWireless Wireless Controller Configuration**

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

### **Version Supported**

Policy Manager only supports Wireless Controller version 8.01.03 and higher.

### **Policy Rules**

This section describes wireless controller support for policy rules.

## *Supported Rule Types*

The Wireless Controller supports the following traffic classification rule types:

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

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

## *"No Change" Filter Sets*

The wireless controller allows administrators to define policies that do not have any filters of their own, but which instead use the set of filters already assigned to a station by a previously applied policy. This type of policy is said to have a "No Change" set of policy rules. Policy Manager does not support policies that have "No change" policy rule sets. Using the ExtremeWireless Wireless Assistant, you will need to remove any policies containing "No Change" rule sets before the wireless controller can be managed by Policy Manager.

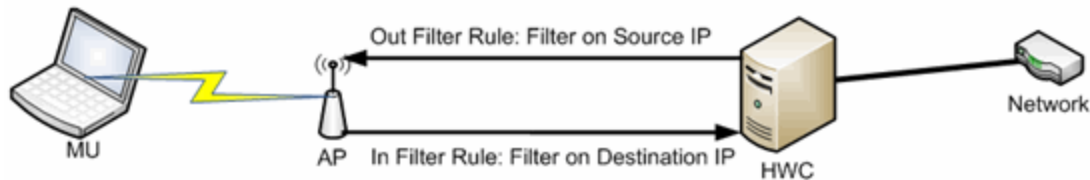
## *Rule Actions*

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

- Access Control: Permit, Deny, and Contain to VLAN actions are supported.
- Class of Service is supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.

## Rule Directions

Policy Manager rules are applied to incoming data packets based on the source or destination address, whereas the wireless controller applies rules to packets based on In/Out direction. On the wireless controller, "In" means coming from the station into the network and "Out" means going from the network out to the station. The wireless controller applies rules to the destination address of inbound packets and to the source address of outbound packets, as shown in the illustration below.



When you create a rule in Policy Manager that allows traffic to a specific destination, that same rule permits data flow from the destination back to the traffic source. This means that Destination rules in Policy Manager map to In/Out rules on the wireless controller. Certain Policy Manager rule types do not have a Source or Destination designation (such as ICMP); however, these rules still map to In/Out rules on the wireless controller to indicate the filters are applied to traffic in both directions. Unchecking the In or Out flag for non-directional rules via the ExtremeWireless Wireless Assistant does not affect the way it is reported to Policy Manager. As long as the rule still exists, verify will succeed.

All rules enforced from Policy Manager are created as "In" rules, and "Out" rules created on the controller are not reported to Policy Manager.

When the egress policy feature is enabled for a VNS, egressing traffic is applied to the defined "In" filters as a "reflected" Out rule (with the source and destination fields reversed) and any explicitly defined "Out" filters created on the controller are ignored. Egress policy may be enabled per VNS by selecting Port Properties for that VNS.

The wireless controller reports to Policy Manager any rules created directly on the controller that contain an "In" component. "Out" rules are not reported to Policy Manager. This allows administrators to define and use "Out" rules on the wireless controller in special cases where additional restrictions need to be imposed.

### *Rule Limits*

The wireless controller has a limit of 64 rules per policy role if the policy is enforced at the controller (bridged @ wireless controller or routed topology), and 32 rules per policy role if the policy is enforced at the AP (bridged @ AP).

## **Role Default Actions**

The following list defines the wireless controller support for role default actions:

- Access Control: Permit, Deny, and Contain to VLAN are supported.
- Class of Service: Inbound and outbound rate limits are supported. 802.1p Priority, and ToS/DSCP Marking are supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.
- The wireless controller will reject policy configurations that specify a VLAN that does not have an egress port already specified.

## **Class of Service**

The following list defines the wireless controller support for Class of Service (CoS) configuration via Policy Manager:

- Inbound and outbound rate limits are supported at the role-level as Class of Service default actions.
- User-based inbound/outbound rate limits are supported for the Default port group for wireless controllers only.
- 802.1p Priority configuration is supported.
- ToS/DSCP Marking is supported.
- TCI Overwrite is not supported.
- Transmit Queue Rate Shaping is not supported.

### *Rate Limits*

The wireless controller supports inbound and outbound rate limits at the role-level as Class of Service (CoS) default actions. There are three states supported for a rate limit:

- Rate limit traffic at the specified rate.
- No Change (the CoS does not specify a rate, and the rate limit is "inherited" from the port's default role or from the global default policy, if one is defined.)

To explicitly prevent traffic from being rate limited for a role, you can map a rate limit with a value of 0 to a CoS, and set that as the default CoS for the role.

## Internal VLAN

The wireless controller uses an *internal VLAN* for processing traffic. For controllers with firmware version 8.01.xx, the internal VLAN is set by default to use VID 1 and the static name of "DEFAULT VLAN." For controllers with firmware version 8.11.xx and later, the internal VLAN uses the VID 4094 and the static name of "INTERNAL VLAN."

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

You can use the Web UI (<https://<controller IP>:5825> > VNS Config > Topologies > Internal VLAN) to change the internal VLAN to a different value, but your policy domain must not use that new value or the Policy Manager enforce will fail.

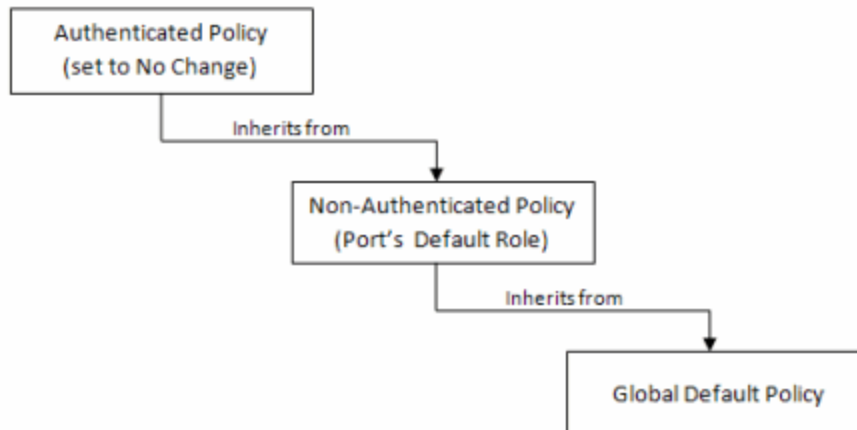
---

**NOTE:** For controllers with firmware version 8.01.xx. Since using a Default VLAN with a VID of 1 is valid on wired devices, the controller's internal VLAN must be changed to another value to prevent issues with Policy Manager enforcing a configuration that uses this VLAN.

---

## Policy Inheritance

The wireless controller uses the concept of policy inheritance, which specifies that if the authenticated policy's access control (VLAN) or class of service (CoS) is set to "No Change," then the policy inheritance hierarchy is used to determine the VLAN and/or CoS. The policy inheritance hierarchy is as follows:



If the authenticated policy's VLAN and CoS are set to "No Change," then the VLAN and CoS settings for the port's default role is used. If the port's default role does not specify the VLAN and CoS, then the global default policy (specified via the ExtremeWireless Wireless Assistant) is used. (In wireless controller terminology, a VNS port's default role is the VNS's default policy.)

It is important to note that Policy Manager does not support "No Change" rules (filter set). If any policy's rules (filter set) are set to "No Change," then Policy Manager is not able to manage the device until the policy containing the "No Change" configuration is removed.

## Configuring RADIUS Servers

When configuring RADIUS authentication and accounting servers, keep in mind the following differences:

- The "Number of Retries" and "Timeout Duration" settings for RADIUS authentication servers are configured on a per-server basis for wireless controller devices. For all other devices, these settings are global to all RADIUS servers, and are specified per device as client defaults.
- The "Update Interval" setting for RADIUS accounting servers is configured on a per-server basis for wireless controller devices. For all other devices, this setting is global to all RADIUS servers, and is specified per device as client defaults.
- For wireless controller devices, the Client Status (Enabled or Disabled) is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. For all other devices, Client Status is configured for each

device, allowing you to enable and disable communication between the device and the RADIUS servers.

- If Strict Mode is enabled, up to three RADIUS servers are automatically associated to each WLAN service. If Strict Mode is disabled, RADIUS servers must be manually added to a WLAN service via the ExtremeWireless Wireless Assistant.

### Other Considerations

- The wireless controller does not support authentication configuration.
- The wireless controller does not support viewing user sessions in the Port Usage tabs.
- The wireless controller must have any VLANs used in a Role's default action already defined on the device and configured with an egress port. If Policy Manager enforces a domain configuration to the wireless controller using a VLAN that does not have an egress port specified, enforce will fail.

# Getting Started with Policy Manager

---

Getting Started with Policy Manager gives you an overview of Policy Manager, and provides a quick tour of its components using the Default Policy Domain. It also includes a summary of the basic steps you must perform to create and configure policies with Policy Manager.

Because Getting Started is meant to be used side-by-side with Policy Manager, it will be most useful if you install Policy Manager first. Once Policy Manager is installed, you can use the steps and suggestions below as an aid in planning and implementing your network policy profiles using Policy Manager.

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

- Installation
- Release Notes
- **Getting Started with Policy Manager** (this guide)
- [Authentication Configuration Guide](#)
- [Policy Manager Concepts](#)

This guide includes the following information:

- [Policy Manager Overview](#)
- [Quick Tour](#)
- [Where to Go from Here](#)

## Policy Manager Overview

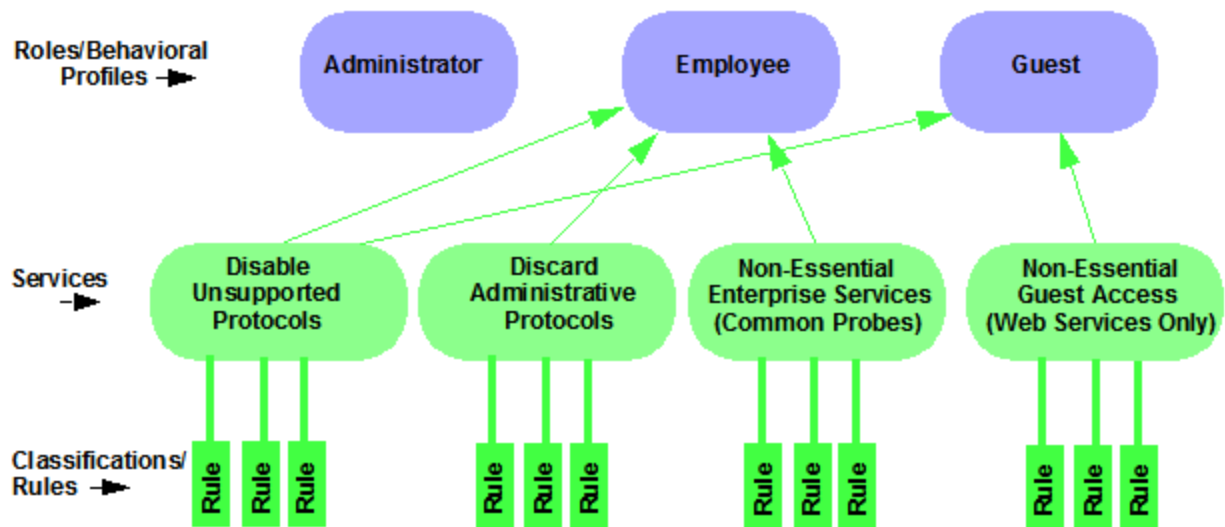
NetSight Policy Manager is a configuration tool that simplifies the creation and enforcement of policies on networks, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

Policy Manager enables you to create policy profiles, called roles, that are assigned to the ports in your network. These roles are based on the existing business functions in your company, and consist of services that you create, made up of traffic classification rules. Roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization.

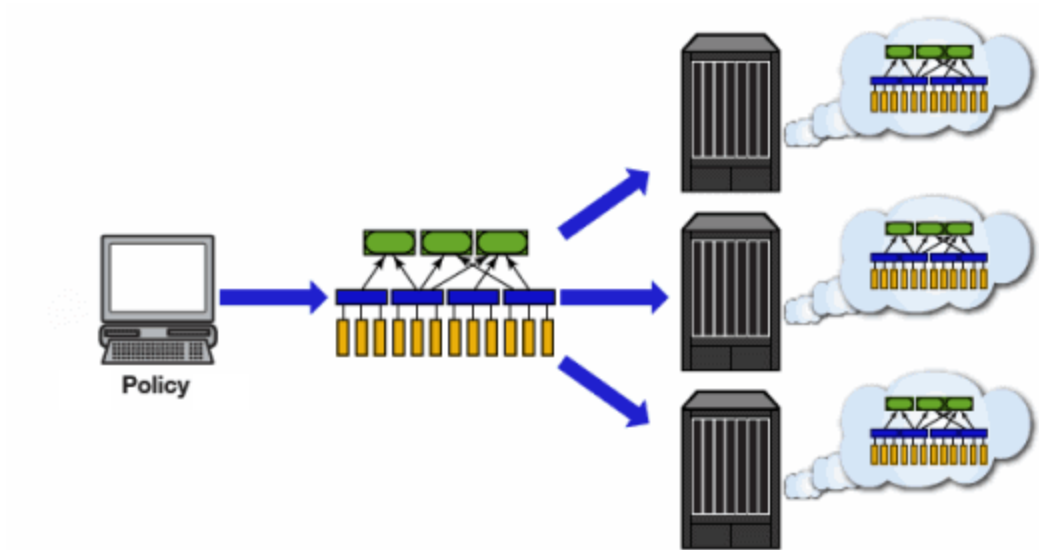


Policy Manager provides [authentication](#) via a RADIUS server to identify users at the time they log in to the network. Only after users have been authenticated are they given customized access capabilities based on the role they are assigned.

The illustration below shows the Policy Manager relationship hierarchy, with Rules at the base to define specific packet handling behaviors, Roles at the top to identify specific job functions in the organization, and Services in the middle, providing the interface between the two layers.



Using Policy Manager wizards and configuration tools, you can create multiple roles tailored to your specific needs, and set a default policy for some or all of your network devices and ports. These policies can be deployed on multiple devices throughout your switch fabric. Once the network infrastructure has been empowered to enforce the relationship hierarchy, no further communication with the Policy Manager application is needed.



## Quick Tour

The Quick Tour will acquaint you with Policy Manager by associating the concepts and features presented here with something you can actually see in the application. While the Quick Tour does not explain all of Policy Manager's features, it shows you how to do some of the basic Policy Manager operations. Links to more detailed instructions for performing basic and more complex Policy Manager tasks are provided throughout the Quick Tour. As you get into the Quick Tour, you will notice that each section of the tour begins with an explanation in regular type, followed by the actual steps you perform, highlighted.

The Quick Tour assumes that you have installed and launched Policy Manager. It also assumes you have installed and launched NetSight Console, and performed a Console Discover to populate the NetSight Database with your network devices. Refer to the Console online Help for information on performing a Discover operation.

By default, when Policy Manager opens, the main window is displayed using the "Consolidated Tab Configuration." In the Consolidated Tab Configuration, there are two left-panel tabs: Roles/Services and Network Elements/Port Groups. Access Control and Class of Service tabs are launched in separate configuration windows from the Edit menu. The Quick Tour is written according to this tab configuration. For more information on available Tab Configurations, see the [Tab Configuration Option](#) Help topic.

The Quick Tour covers the following features:

- [Understanding Policy Domains](#)
- [Understanding Roles](#)
- [Understanding Services](#)
- [Working with Service Groups](#)
- [Understanding Traffic Classification Rules](#)
- [Adding Devices](#)
- [Configuring Devices for Authentication](#)
- [Working with Device Groups](#)
- [Viewing Port Configuration Information](#)
- [Working with Port Groups](#)
- [Working with VLANs](#)
- [Viewing Classes of Service](#)
- [Using Policy Manager Wizards](#)
- [Saving the Domain](#)
- [Enforcing](#)
- [Accessing Policy Manager Help](#)

## Understanding Policy Domains

Policy Manager provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between Policy Manager clients.

The first time you launch Policy Manager, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. The Default Policy Domain is pre-configured with a Policy Manager Database file called Demo.pmd. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and will often need customization to fully leverage the power of a policy-enabled network.

For more information about domains, see [Policy Domains](#) in the Concepts Help topic.

In the Quick Tour, we'll use the Default Policy Domain as a way to explore the basic features and functionality of Policy Manager. Later, you may find the Default Policy Domain useful as you create your own Policy Domains.

If you have just launched Policy Manager for the first time, you are in the Default Policy Domain and you can proceed to the next step, [Understanding Roles](#). If someone else has been using Policy Manager before you, use the following steps to create a Demonstration Domain that you can use for the Quick Tour.

**Note:** If someone else has been using Policy Manager before you, when you create the new domain, you may be prompted to save the previous domain's configuration.

### Quick Tour: Creating a Policy Domain.

1. Select **Domain > Create Domain**. Enter the domain name **Demonstration Domain** for the new domain and click **OK**. The new Demonstration Domain opens.
2. Select **File > Import > Import From File**. The Import from File window opens.
3. Click the **Browse** button and select the Demo.pmd file. Click **Open**.
4. Click the **Select All** button to select all the data elements to import.
5. Click **OK**. The data elements will be imported from the Demo.pmd file into the new Demonstration Domain.

When you selected the Demo.pmd, you probably noticed that there are many .pmd files to select from. These different files are pre-configured domains that include roles, services, and rules designed for specific network scenarios.

For more information:

- [How to Create and Use Domains](#)

Now that you've created the Demonstration domain, we will explore Policy Manager in a little more depth.

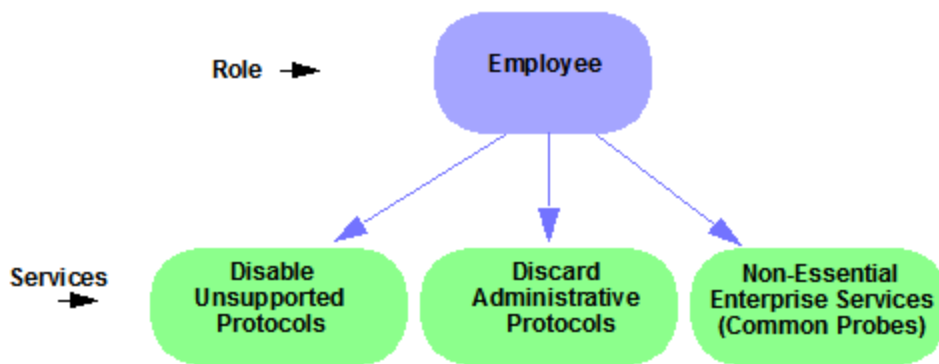
## Understanding Roles

Roles are usually designed to reflect different users in your organization and to provide customized access capabilities based on the role users have in your organization. For example, accounting and engineering personnel have different network access and priority needs and therefore might have different roles.

### Quick Tour: Checking out roles.

1. Click on the left-panel Roles tab in the Policy Manager main window.
2. Hold the cursor over a role name to see a tooltip describing the role.
3. Click on the various roles listed in the left panel, and in the right panel you'll see tabs that display specific information for each role. Click the right-panel tabs to see the information they contain.

A role can be made up of one or more network access services that are defined in Policy Manager. These services determine how network traffic will be handled at any network access point configured to use that role. A role may also contain default access control (VLAN) and/or class of service designations that will be applied to traffic not handled specifically by the services contained in the role. A role can contain any number of services or service groups.



Roles are assigned to users during the authentication process. When a user successfully authenticates, the port is opened, and if there was a role assigned to the user, that role is applied to the port. A role can also be directly assigned to a port as a default role for instances when authenticated users are not assigned a role. If an end user on a port was not assigned a role when logging in (authenticating), or if authentication is inactive on a port, then the port's default role will take effect. However, if a user is assigned a role upon login, then that role will override any default role on the port.

To create and define a role, you can use the [Role Wizard](#) or do it using the right-panel Role tabs.

Right now, we will just create and name a role without defining it further:

**Quick Tour: Creating a role.**

1. In the Policy Manager left panel, select the Roles tab.
2. Right-click the Roles folder, and select Create Role.
3. Enter the role name **Office Assistant** in the highlighted box and press Enter.

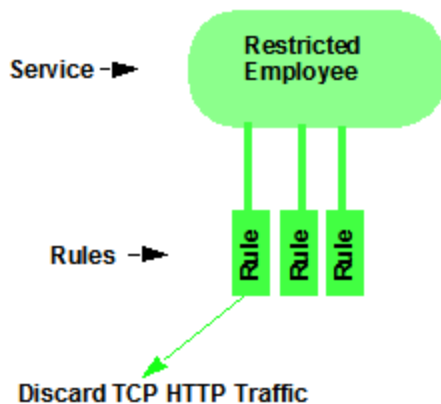
For more information:

- [Role](#)
- [How to Create a Role](#)

## Understanding Services

Roles can be made up of one or more network access services. These services determine how network traffic will be handled at any network access point configured to use that role. Policy Manager allows you to create Local Services (services that are unique to the current domain) and Global Services (services that are common to all domains). Services can be one of two types: Manual Service or Automated Service. Manual services contain customized classification rules that you create, while Automated services are associated with a particular set of network resources.

Manual services contain one or more traffic classification rules that define how a network access point will handle traffic for a particular network service or application. For example, you might create a Manual service called "Restricted Employee" that contains a classification rule that discards TCP HTTP traffic.



We will create a Manual service and add it to a role later on. Right now, we'll just take a look at the services in the domain.

### Quick Tour: Checking out Services.

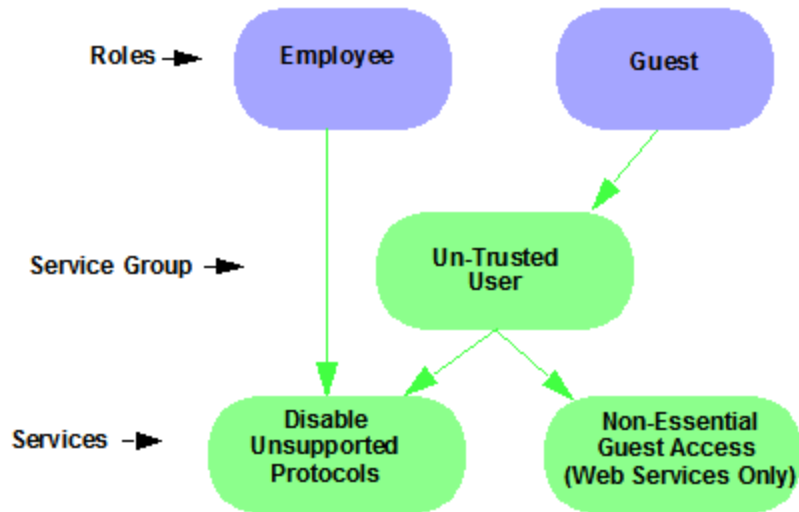
1. Click on the left-panel Services tab in the Policy Manager main window.
2. Expand the Service Repository folder and then the Local Services folder.
3. Expand the Services folder to view a list of services.
4. Hold the cursor over a service name to see a tooltip describing the service.
5. Expand a service or two to see the individual classification rules that make up the service.
6. Select a service or two in the left panel to see the right-panel tabs that display specific information for each service. Click the right-panel tabs to see the information they contain.

For more information:

- [Service](#)
- [How to Create a Service](#)

## Working with Service Groups

Services can be grouped together into Service Groups. This allows you to easily add a set of services to one or more roles.



### Quick Tour: Checking out Service Groups.

1. Click on the left-panel Services tab in the Policy Manager main window.
2. Expand the Service Repository folder and then the Local Services folder. Expand the Service Groups folder.
3. Expand the Acceptable Use Policy service group to see its services. Note that these services are also listed under the Services folder.

After you have defined and created your services, you can easily create a Service Group and then drag and drop your services into the group.

### Quick Tour: Creating a Service Group.

1. Click on the left-panel Services tab in the Policy Manager main window.
2. Expand the Service Repository folder and then the Local Services folder.
3. Right-click the Service Groups folder, and select Create Service Group.
4. Enter the service group name **Trusted User** in the highlighted box and press **Enter**.
5. Drag and drop one or two of the existing Acceptable Use Policy services from the Acceptable Use Policy service group into the Trusted User service group. Notice that this makes a copy of the existing service in the new folder.

For more information:

- [How to Create a Service Group](#)



## Understanding Traffic Classification Rules

Traffic Classification rules allow you to assign access control (VLAN membership) and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, and 4 of the OSI model, and all network traffic can be classified according to specific layer 2/3/4 information contained in each frame.

A Traffic Classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the traffic classification type for the rule. Actions apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

You create a rule for a specific service, but a rule can be added to multiple services simply by using drag and drop to copy the rule from one service to another in the Services tab.

### Quick Tour: Checking out Rules.

1. In the left-panel Services tab, expand the Acceptable Use Policy service group.
2. Expand the Deny Unsupported Protocol Access service and click on the Discard AppleTalk rule.
3. Click on the right-panel General tab to see the rule's Traffic Description and Actions.
4. Use the Edit button to add a description to the General Tab, for example: **AppleTalk not supported on this network.**

For more information:

- [Rule](#)
- [Traffic Classification Rules](#)
- [How to Create or Modify a Rule](#)

## Adding Devices

The first step in adding network devices to Policy Manager, is to add the devices to the NetSight database. You do this initially, by performing a Console Discover to populate the database, or by using Console to import devices from a .ngf file.

We will assume that you have already done this. If you need more information, refer to your NetSight Console online Help.

Once devices have been added to the NetSight database, you must assign the devices to a [Policy Domain](#) using Policy Manager. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy Manager device tree. Only devices assigned to the domain you are currently viewing are displayed.

#### Quick Tour: Assigning Devices to a Domain.

1. In the Policy Manager main window, select **Domain > Assign Devices to Domain**. The Assign Devices to Domain window opens.
2. In the left panel, the Unassigned device tree contains all the devices in the database that have not been assigned to a domain. The right panel displays the devices in the current domain.
3. For the Quick Tour, select a couple of devices to add to the domain and click **Add**. Click **OK** to add the devices.
4. You can also use this window to remove a device from the current domain. This removes the device from the current domain and places it in the Unassigned folder. It does not delete the device from the NetSight database.

After you have initially added your devices, you can use Policy Manager's Add Device window to add a single device to the database. Adding a device this way also automatically adds it to the current domain.

For more information:

- [How to Add and Delete Devices](#)
- [How to Create and Use Domains](#)

## Configuring Devices for Authentication

Now that you have added devices to your domain, you can configure them for authentication. In Policy Manager, several types of authentication are offered, including Web-based, 802.1X, MAC, and CEP authentication. In order to take advantage of the authentication features of Policy Manager, you need to configure your network and your devices to work with a RADIUS server. In the Quick Tour, we will take a look at the right-panel tabs where you can view and modify authentication and RADIUS configuration on devices.

### Quick Tour: Viewing the Authentication Settings on a Device.

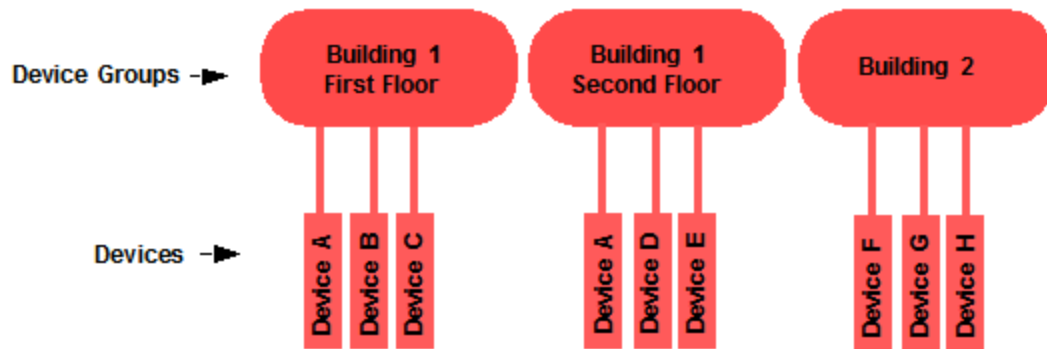
1. In the Policy Manager left panel, select the Network Elements tab.
2. Expand the All Devices folder and select a device.
3. In the right panel, look at the Details View tab. Expand a Ports or Slot folder to see ports on the device. Scroll to the right to see all the port information available on this tab.
4. Select the right-panel Authentication tab. This tab is where you specify the authentication type, enable or disable authentication, and configure your authentication settings for the selected device.
5. Select the RADIUS tab. On this tab you can enable the device as a RADIUS client, and set up communication between the RADIUS client device and the RADIUS server.

For more information:

- [Authentication](#)
- [Authentication Configuration Guide](#)
- [How to Configure Devices](#)

## Working with Device Groups

In the Network Elements tab, devices are listed individually, but they are also grouped into Device Groups. This can be useful when you want to configure policies for a group of devices. An example of how devices could be grouped is shown here.



Policy Manager provides several system-created device groups for your convenience. When a device is assigned to a domain, it automatically becomes a member of the appropriate group:

- All Devices - contains all the devices that are assigned to the current domain.
- Grouped By - contains five subgroups:
  - Chassis -- contains subgroups for specific chassis in the domain.
  - Contact -- contains subgroups of the devices in a domain based on the system contact.
  - Device Types -- contains subgroups for the specific product families and device types in the domain.
  - IP -- contains subgroups based on the IP subnets in the domain.
  - Location -- contains subgroups of the devices in a domain based on the system location.

You can also create your own device groups, called user-defined device groups. Policy Manager system-created device groups are displayed with blue folders. Any group you add will be displayed with a yellow folder.

For more information:

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

## Viewing Port Configuration Information

After devices have been imported into Policy Manager, you can view and configure their ports by selecting a device and displaying its ports in the right-panel Details View tab or Ports tab.

### Quick Tour: Viewing Port Configuration Information.

1. Click on the left-panel Network Elements tab in the Policy Manager main window.
2. Expand the All Devices folder and select a device.
3. In the right-panel Details View tab, expand a Ports or Slot folder to display ports on the device.
4. Right-click on a port and select Properties. The Port Properties window opens.
5. Take a look at all the tabs where you can view and modify configuration information for the selected port.

For more information:

- [How to Configure Ports](#)

## Working with Port Groups

Policy Manager allows you to group ports into User-Defined Port Groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, at the same time. Policy Manager also provides you with Pre-Defined Port Groups. Every time one of the Pre-Defined Port Groups is accessed, Policy Manager goes to the devices in the current domain and retrieves the ports which fit the pre-defined characteristics of the port group.

### Quick Tour: Checking out Pre-Defined Port Groups.

1. Click on the left-panel Port Groups tab in the Policy Manager main window.
2. Expand the Port Groups folder.
3. Expand the Pre-Defined Port Groups to see the groups.

### Quick Tour: Creating a User-Defined Port Group.

1. Expand the Port Groups folder.
2. Right-click the User-Defined Port Groups folder, and select Create Port Group.
3. Type in a Port Group name in the highlighted box and press **Enter**.

4. Look at the Ports tab in the right panel. Notice that you can add a description of the port group and add individual ports to the group.

For more information:

- [How to Create a Port Group](#)
- [Pre-Defined Port Groups](#)

## Working with VLANS

All traffic in a Policy Manager network is assigned membership in a VLAN. Roles are used to assign VLAN membership to traffic either through the role's default access control or through the role's services which may include traffic classification rules that assign VLAN membership (access control).

When you open a new domain, the Global VLANs folder is prepopulated with the Default VLAN (not to be confused with a default VLAN that is assigned to a role, although the Default VLAN *could* be a default VLAN for a role). You can then create additional VLANs and assign them as default access control for a role and/or use them to define traffic classification rules. You can view the roles and services associated with a VLAN using the Role/Service Usage window accessed by right-clicking on a VLAN. You can also make role and service changes from this window.

Island VLANs are used in Policy VLAN Islands, which enable you to deploy a policy across your network, while restricting user access to only selected local devices. You must select the Policy VLAN Islands Enabled checkbox (on the Edit Menu) to see the Island VLANs folder and the Policy VLAN Islands folder.

### Quick Tour: Checking out VLANs.

1. From the Policy Manager Edit menu, select Access Control Configuration. The Access Control Configuration window opens.
2. In the left panel, expand the Global VLANs folder to see the individual VLANs.
3. Click on the Default VLAN listed and view the General tab in the right panel.

For more information:

- [How to Create a VLAN](#)
- [General Tab \(VLAN\)](#)

- [Policy VLAN Islands](#)

## Viewing Classes of Service

Policy Manager lets you create a class of service (CoS) that includes one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default.

### Quick Tour: Checking out Classes of Service.

1. From the Policy Manager Edit menu, select Class of Service Configuration. The Class of Service Configuration window opens.
2. Notice that the window is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS/DSCP, drop precedence, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own classes of service (user-defined CoS).
3. Scroll to the right to see that you can also use this window to define inbound and outbound rate limits and outbound transmit queue rate shapers for your classes of service.
4. Click on the Table Display Filter button to see a menu that lets you specify which columns you would like displayed in the table. For example, if you want to view the inbound rate limits that are configured, you can select to display only Inbound RL, making it easier for you to focus in on the desired information.
5. Click on the Domain Managed CoS Components button to see a menu you can use to specify the CoS components you will be configuring for this domain. This will determine what CoS settings will be written to your network switches on Enforce. For example, if you select only Inbound RL and Outbound RL, then Policy Manager will enforce the rate limits you configure, but will not overwrite any transmit queue settings configured on the device via the Command Line Interface (CLI).

For more information:

- [Getting Started with Class of Service](#)
- [How to Define Rate Limits](#)

- [How to Configure Transmit Queues](#)
- [How to Create a Class of Service](#)

## Using Policy Manager Wizards

In Policy Manager, you can create roles, services, rules, and VLANs, and configure devices and ports, by selecting the appropriate item in the left panel and filling out the right-panel tabs. But Policy Manager also provides wizards that lead you through the steps required to perform these functions.

If you are creating roles, services, and rules, and configuring devices and ports from scratch, the wizards can be easier to use. Once you've created everything you need, you may find it easier to make changes and additions on the right-panel tabs, or you may still want to use the wizards, depending on the situation.

The wizards provided by Policy Manager include the Role Wizard, the Service Wizard, the Classification Rule Wizard, the Device Configuration Wizard, the Port Configuration Wizard, and the Policy VLAN Islands Configuration Wizard. The Service Wizard incorporates the elements of the Classification Rule Wizard, and the Role Wizard incorporates the elements of the Service Wizard, including the Classification Rule Wizard.




In the Quick Tour, we will use the Service Wizard to create a Manual service that includes one classification rule. We will then apply it to the role you created earlier in the Quick Tour.

### Quick Tour: Creating a Service Using the Service Wizard.

Let's create a service that discards TCP HTTP traffic.

1. In the Policy Manager left panel, select the Services tab.
2. Expand the Service Repository folder and then the Local Services folder.
3. Right-click the Services folder, and select Service Wizard.



4. Enter **Restricted Employee** for the service name and click **Next**.
5. Make sure the Service Type selected is Manual, and click **Next**.
6. Enter **Discard HTTP** for the classification rule name and click **Next**.
7. Choose Enabled as the Rule Status and click **Next**.
8. Choose All Devices as the Rule Type and click **Next**.
9. Leave the TCI Overwrite Status as Disabled and click **Next**.
10. Choose Layer 4 - Application Transport as the Traffic Classification Layer, and click **Next**.
11. Choose IP TCP Port Destination as the Traffic Classification Type and click **Next**.
12. Choose Well-Known Values and HTTP (80) as the TCP Type and click **Next**.
13. Adding an IP Address is optional, so just click **Next**.
14. Select the Deny Traffic option from the Access Control drop-down list. Click **Next**.
15. View the Classification Rule Summary and click **Next**.
16. Select the role you created earlier (Office Assistant) and click **Finish**.
17. Look at the right side of the Status Bar at the bottom of the window. The Enforce icon  means your new role and its service need to be enforced (written to the devices). We'll talk about that later.

For more information:


- [Using the Service Wizard](#)
- [Using the Classification Rule Wizard](#)
- [Using the Device Configuration Wizard](#)
- [Using the Port Configuration Wizard](#)
- [Using the Role Wizard](#)

## Saving the Domain

After a Policy Domain has been changed, you must save the domain to notify all clients that are viewing that domain of the change and automatically update

their view with the new configuration. A Save icon is displayed in the status bar at the bottom of the main window when you have made changes to the domain that need to be saved.

### Quick Tour: Saving the Domain.


1. Note that a Save icon  appears on the status bar. This is a reminder that you need to save changes you've made to the domain.
2. From the menu, select **File > Save Policy Domain**.
3. The domain is saved and all clients viewing the domain will automatically have their view updated with the new configuration.

For more information:

- [How to Create and Use Domains](#)

## Enforcing

Any time you add, make a change to, or delete a role or any part of it (any of its services and/or rules), the devices in your current domain need to be informed of the change so that your revised policy configuration can take effect. This is accomplished by enforcing -- writing your policy configuration to a device or devices. Enforce operations are performed only on the current domain.

To enforce to all devices in the current domain, you would use the Enforce button in the toolbar or the **File > Enforce Role Set** menu option. To enforce to a single device, you would right-click the device and select Enforce Role Set from the menu. If you have made any changes that need to be enforced, the Enforce icon  appears on the status bar at the bottom of the Policy Manager window as a reminder.

Policy Manager's Enforce Preview window enables you to view the information that will be written to your domain devices, before you actually enforce. This feature is particularly useful if you have devices that only support certain aspects of policy management. The Enforce Preview window appears whenever you initiate an enforce using one of the methods mentioned above, so that you always have a chance to review the effects of enforcing prior to actually performing the enforce. You can also access this window from the **File > Enforce Preview** menu option.

To determine if the roles currently in effect on your domain devices match the set of roles you have defined in your current Policy Domain configuration, use the [Verify](#) feature.

### Quick Tour: Enforce Preview.

At this point, you probably don't want to actually enforce to the devices in the domain. So let's just look at the Enforce Preview window.

1. Select **File > Enforce Preview**. The Enforce Preview window opens. Use the tabs in the window to check out all the information that would be written to your devices if you did perform an enforce.

For more information:

- [Enforcing](#)
- [Enforce Preview Window](#)
- [Verifying](#)

## Accessing Policy Manager Help

All Policy Manager documentation is available in the Help system accessible from the application. To launch the NetSight Suite Online Help, select **Help > Help Topics** from the Help menu.

- Help on Policy Manager 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.
- Help for a particular window is also available via a **Help** button on the window itself.

The Help system includes a Search feature that lets you search for specific instances of a term in all the help topics.

### Quick Tour: Using the Help Search Feature.

1. Select the **Help > Help Topics** menu option. The NetSight Suite Online Help opens in a web browser.
2. In the left-panel you will see the Table of Contents that displays all the help topics for the NetSight Suite application.
3. At the bottom of the Table of Contents you will see a tab for **Search All**

### Topics and Favorites.

4. Click the **Search All Topics** tab. In the Search field, enter the word "role" and press **Enter** or click the **Search** button. A list of topics in which the term appears is displayed, along with the number of instances found in each topic. If you want to find a specific combination of words that are always next to each other in the same order, enter the search keywords within quotation marks (for example, "domain name").
5. The Search feature lets you refine the Search results by using the Filters drop-down menu to select which NetSight application's Help topics you are interested in searching. Use the drop-down menu to select the Policy Manager filter.

---

**TIP:** There is also a search field in the Help toolbar lets you search for a term only on the topic that is currently displayed.

---

## Where to Go from Here

If you have been following the [recommended reading sequence](#), your next stop will be the [Authentication Configuration Guide](#). If you've already done that, and have read the other recommended reading, then you are ready to start implementing your own policy configurations using Policy Manager.

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

1. Configure your network for authentication (see the [Authentication Configuration Guide](#).)
2. Create your Policy Domains (see [How to Create and Use Domains](#).)
3. [Add your devices](#) to the NetSight Database and assign them to the appropriate domain.
4. Configure authentication on devices and ports (see [How to Configure Devices](#) and [How to Configure Ports](#)).
5. If desired, group your ports into port groups (see [How to Create a Port Group](#)).
6. Create services (see [How to Create a Service](#)).
7. If desired, group services into service groups (see [How to Create a Service Group](#)).

8. Create roles (see [How to Create a Role](#)).
9. Write your configuration to your devices (see [Enforcing](#)).

Now that you have set up your authentication and policy configuration, you can start exploring some of Policy Manager's other features:

---

• Define Authorization and Device Access	<p>Use the Authorization/Device Access window to configure your Policy Manager access privileges. The window has four tabs:</p> <ul style="list-style-type: none"><li>• Users/Groups tab lets you manage user access to specific features and capabilities.</li><li>• Profiles/Credentials tab lets you define SNMP <i>credentials</i> used to access your network devices, and create <i>profiles</i> that use these credentials for various device access levels.</li><li>• Profile/Device Mapping tab lets you specify the <i>profiles</i> that will be used by users when communicating with network devices.</li><li>• Manage SNMP Passwords tab where you can manage the <i>credentials</i> that have been set on your network's devices.</li></ul>
• <a href="#">Server Locks</a>	<p>Policy Manager uses Server Locks to manage interactions between multiple clients and the server. When a user begins editing a Policy Domain, a lock is acquired for that domain at the server. That lock is not released until the same user saves the domain data. This guarantees a consistent view of that domain for all clients.</p>
• Server Information	<p>The Server Information window lets you view and configure certain NetSight Server functions, including management of client connections, database backup and restore, locks, and licenses. It also provides access to the server log and server statistics.</p>
• <a href="#">Options</a>	<p>Use the Options window to set options for NetSight functions on a suite-wide and per-application basis.</p>
• <a href="#">Class of Service</a>	<p>Policy Manager supports Class of Service (CoS), which allows you to assign priority, modify rates, and change transmit queue behavior for your network traffic.</p>

---

- 
- [Network Resource Groups](#) Network Resource Groups are groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. You can create a network resource group and associate it with an [Automated service](#). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource address in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.
- 
- [Policy VLAN Islands](#) Policy Manager offers you the ability to set up Policy VLAN Islands which enable you to deploy a policy across your network, while restricting user access to only selected local devices.
- 
- **Web Update** Policy Manager provides an easy way to access and download product updates using a web update operation. You can perform an immediate check for updates, or schedule a routine check for updates.
- 

## Related Information

For information on related concepts:

- [Policy Manager Concepts](#)
- [Traffic Classification Rules](#)

For information on related tasks:

- [Authentication Configuration Guide](#)

For information on related windows:

- [Main Window](#)

# Configuring Authentication

---

Authentication is the process by which end users identify themselves to the network and are given customized access capabilities based on the role they serve in the organization. Policy Manager supports the following different types of authentication: Web-based, 802.1X, MAC, CEP, Quarantine, and Auto Tracking. For more information on the different types of authentication, see [Authentication Types](#).

To assist you in configuring authentication for your network, Policy Manager provides an Authentication Configuration Guide that presents steps for configuring the various components required for authentication. In addition, several configuration supplements provide information specific to different types of authentication. It is recommended that you begin by following the instructions in the Authentication Configuration Guide, then refer to the supplements for additional information, if applicable to your type of authentication.

The following Authentication Configuration Help topics are provided:

- [Authentication Configuration Guide](#)
- [802.1X Authentication Configuration Supplement](#)
- [Configuring a Windows Server 2000 or 2003 for RADIUS Authentication](#)
- [Configuring a Windows Server 2008 for RADIUS Authentication](#)
- [Configuring Quarantine Authentication](#)
- [Configuring Auto Tracking Authentication](#)

# Authentication Configuration Guide

---

Authentication is the process by which end users identify themselves to the network and are given customized access capabilities based on the role they serve in the organization. Policy Manager uses a RADIUS server and an authentication-enabled device to dynamically assign a policy (role) to a port, based on the end user's login or MAC address.

Policy Manager supports the following types of authentication: Web-based, 802.1X, MAC, CEP, Quarantine, and Auto Tracking. (For more information on each type, see the [Authentication](#) section in the Policy Manager Concepts Help topic.) This guide presents steps for configuring the various components required for authentication, and, if necessary, refers you to additional [configuration supplements](#) that provide information specific to the different types of authentication.

Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User Authentication). Refer to the NetSight Firmware Support tables for information on the authentication types supported by each device type.

While most of the main configuration tasks can be performed in any order, the recommended sequence is below. When you have completed the configuration tasks, a test user should be able to authenticate on the network and be assigned the correct role.

In order to configure your setup for authentication, you will need the following components:

- NetSight Policy Manager
- RADIUS authentication server and user interface
- Policy-enabled devices (switches)
- Hardware for running Policy Manager and the RADIUS Server

You may already have these components installed and running, but you should read all the sections of this document anyway, as they contain information that will help you to configure them for use with Policy Manager. You may want to perform your initial configuration in a test environment before deploying it on your network.



**NOTES: Configuring Windows Server 2008**

Users of Windows Server 2008 should read this Authentication Configuration Guide, but should follow the steps in [Configuring a Windows Server 2008 for RADIUS Authentication](#) for instructions on installing and configuring the RADIUS server.

**Configuring Windows 2000 Advanced Server and Windows Server 2003**

Users of Windows 2000 Advanced Server and Windows Server 2003 should read this Authentication Configuration Guide, but should follow the steps in [Configuring a Windows Server 2000 or 2003 for RADIUS Authentication](#) for instructions on installing and configuring the RADIUS server.

**Configuring Windows 2000**

Windows 2000 users who plan to utilize Funk Software Inc.'s Steel-Belted RADIUS should consult Funk's website [www.funk.com](http://www.funk.com) for assistance in setting up Steel-Belted RADIUS on Windows 2000, in particular Tech Bulletins RD 410 and RD 447 (look for Tech Support > Steel-Belted Radius > Steel-Belted Radius Tech Notes > View by Tech Note ID Number).

---

## Instructions on:

1. [Preliminary Reading](#)
2. [Installing Policy Manager](#)
3. [Post-Installation Reading](#)
4. [Planning Your Policies \(Roles and Services\)](#)
  - a. [Identifying Roles](#)
  - b. [Defining Services](#)
5. [Planning for Port Mode](#)
6. [Configuring End Users](#)
  - a. [Configuring a Windows Workstation as a DHCP Client](#)
  - b. [Configuring a Linux Workstation as a DHCP Client](#)
  - c. [Browser Requirements for Web-Based Authentication](#)
7. [Installing and Configuring the RADIUS Server](#)
  - a. [Installing the RADIUS Server](#)
  - b. [Adding RADIUS Client Devices](#)
  - c. [Adding RADIUS Users](#)
8. [Configuring RADIUS in Policy Manager](#)
  - a. [Downloading the Firmware](#)
  - b. [Adding Devices to Policy Manager](#)

- c. [Configuring the Port Mode](#)
  - d. [Configuring Devices as RADIUS Clients](#)
  - e. [Configuring Authentication on Devices](#)
9. [Testing Authentication](#)
- a. [Testing Web-Based Authentication](#)
  - b. [Testing 802.1X Authentication](#)

## Preliminary Reading

Before configuring your network for Policy Manager, read as much about Policy Manager and its associated technologies as you can, to familiarize yourself with Policy Manager's features and the business challenges it has been designed to solve. The following reading sequence is advised:

- **RADIUS Vendor Documentation** - Policy Manager utilizes a RADIUS server for authentication. If you do not already have a RADIUS server installed, you will need to install one following your vendor's installation instructions. You will then need to be able to use the RADIUS server user interface to configure the RADIUS server for use with Policy Manager.
- **NetSight Installation** - This topic provides information on the minimum requirements for running Policy Manager, platform-specific information, and instructions for installing the application. The Installation document is available by selecting **Help > Help Topics** from the Policy Manager menu after installation, or on the Network Management Suite (NMS) Documentation web page:  
<http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx>.
- **NetSight Release Notes** - The release notes contain release-specific information, including known issues and any available workarounds. You can access the Release Notes by selecting **Help > Release Notes** from the Policy Manager menu after installation. In addition, the latest version of the release notes are available on the Network Management Suite (NMS) Documentation web page:  
<http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx>.

## Installing Policy Manager

In Policy Manager, you will be setting up communication between your RADIUS server and your Policy Manager devices, and creating the roles that will be mapped to your users in the RADIUS server for authentication purposes.

Although it is not required that you install Policy Manager before installing your RADIUS server, installing Policy Manager as a first step gives you easy access to Policy Manager documentation via the **Help > Help Topics** menu option, and lets you familiarize yourself with the application before doing any actual configuration. To install Policy Manager, follow the Installation instructions.

## Post-Installation Reading

After you've installed Policy Manager, familiarize yourself with the application by selecting **Help > Help Topics** from the menu and reading the following Help topics:

- [Getting Started with Policy Manager](#) - This topic provides a brief overview of Policy Manager and a Quick Tour of its features. It is suggested that you take the Quick Tour before you start creating roles and configuring devices in Policy Manager.
- [Policy Manager Concepts](#) - This topic explains some of the concepts you'll need to understand in order to make the most effective use of Policy Manager, including a section on Authentication that describes the types of authentication that Policy Manager supports, and how authentication works.
- **Configuration Supplements** - These Help topics provide supplemental information for specific authentication types and configurations:
  - [Configuring a Windows Server 2000 or 2003 for RADIUS Authentication](#) -- for users of Windows 2000 Advanced Server or Windows Server 2003.
  - [Configuring a Windows Server 2008 for RADIUS Authentication](#) -- for users of Windows Server 2008.
  - [802.1X Authentication](#) -- configuration information specifically for networks using 802.1X authentication.

After completing this reading, continue with the tasks below.

## Planning Your Policies (Roles and Services)

It is recommended that, prior to performing any configuration tasks, you plan in advance the policy profiles, or "roles," that will be applied to your users. For testing purposes, you do not need to create all the roles at this point, but you should have an idea what some, if not all, of the role *names* are going to be.

The roles you will eventually be creating in Policy Manager are usually named for business functions that already exist in the enterprise. You will create customized services made up of traffic classification rules, that you will apply to your roles. A role may also contain default actions including access control (VLAN) and class of service designations that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any default actions, determine how all network traffic will be handled at any network access point configured to use that role.

If you have not done so already, read the discussion of Roles and Services in [Policy Manager Concepts](#), and the [Traffic Classification Rules](#) Help topic for background. This will assist you in planning your roles, and the services and rules you'll need to create to apply to them.

### *Identifying Roles*

Roles are usually named for a type of user such as Student or Faculty. As you begin identifying potential policy roles within your organization, consider the following issues:

- What are the different users and their network access requirements? For example, do you have some users that require priority access? Do you have other users that should be denied access?
- What are the network service or application priority requirements? For example, is there an application like SAP that requires priority?

After the different roles have been determined, you must determine if each role will have a default access control and whether or not the traffic should be contained to a VLAN or denied. Should there be a default class of service for a role? If so, what should it be?

### *Defining Services*

Once a role has been identified, you need to define the services and rules that will make up that role. It is helpful to establish a naming convention for services where the name describes the service's action. By carefully determining this naming convention, you can facilitate the administration of the policy configuration.

Examples of a naming conventions might be:

- Services that do not deny traffic and don't have a class of service action associated with them are prefixed with the term "Allow" (e.g. "Allow Print Access" or "Allow Email").
- Services that deny traffic are prefixed with the term "Deny" (e.g. "Deny Telnet").
- Services that do not deny traffic and have a priority action associated with them are suffixed with a term denoting the priority of the action (e.g. "External Web (P3)" and "External Web (P7)").

An alternative convention would be to have the "Allow" and "Deny" terms be suffixes so when the services are listed alphabetically, all the different versions of a single service would be listed together.

You should also consider whether there is an advantage to grouping your services into Service Groups. If you will be adding the same group of services to multiple roles, Service Groups will make this task easier.

Once you have defined your required services, you can outline the various classification rules that must be created as the working base of each service. For more information on how classification rules are created and used, see [Traffic Classification Rules](#).

Once you've got an idea of what your roles and services will be, continue with the configuration tasks below.

## Planning for Port Mode

Another issue to be decided in advance is port mode. Port mode determines which ports in your network will require authentication by users, and how you wish unauthenticated traffic to be handled on all ports, whether authentication is active or inactive. See [Port Mode](#) in the Policy Manager Concepts Help topic for more information.

For testing purposes, you do not need to set the port mode on every port, but you should know how you want each port to behave before you implement your policies. We will be setting the port mode on a couple of ports later on in our configuration procedures ([Configuring the Port Mode](#)) for testing purposes.

Once you have an idea of what the port mode settings will be on your ports, continue with the tasks below.

## Configuring End Users

This section deals with configuring the end user. Depending on your setup, you may or may not need to set up your end user workstations as DHCP clients. If you are configuring web-based authentication, the end user must have access to either an Internet Explorer (IE) or Mozilla Firefox browser in order to launch the authentication web page. Use the procedures in this section that are appropriate to your configuration.

### *Configuring a Windows Workstation as a DHCP Client*

To configure a Windows workstation as a DHCP client, you will enable the DHCP protocol and remove the WINS and DNS IP addresses. The procedure may vary slightly, depending on the operating system. The following instructions are for a Windows XP workstation:

1. Launch the TCP/IP Properties window. Select **Start > Settings > Network Connections** and right-click on Local Area Connection to open the Local Area Connection Properties window.
2. Select Internet Protocol (TCP/IP) and click the **Properties** button to open the Internet Protocol (TCP/IP) Properties window.
3. In the General tab, select the "Obtain an IP address automatically" and "Obtain DNS server address automatically" options. Click the **Advanced** button to open the Advanced TCP/IP Settings window.

**NOTE:** The next two steps are required so that the existing IP addresses will not overwrite the addresses obtained by DHCP.

4. In the DNS tab, remove all the values or IP addresses, except for the Host Name.
5. In the WINS tab, remove all WINS IP addresses and check the "Enable LMHOSTS Lookup" box.
6. Click **OK** to close the windows.
7. Reboot the system.
8. To verify that the DHCP server is now providing the IP addresses for the clients, open an MS-DOS window and use the appropriate `ipconfig` command:
  - To view the current IP address: `ipconfig /all`
  - To release the current IP address: `ipconfig /release`

- To renew the current IP address or request a new IP address:  
`ipconfig /renew`

### *Configuring a Linux Workstation as a DHCP Client*

To cause a Linux workstation to request a DHCP address, type the command:

```
/sbin/dhclient
```

in an xterm window where you are logged in as root. This request will not persist if you reboot the workstation.

If you would like to configure DHCP so that it is persistent across reboots, you can use the DHCP configuration tool.

1. In an xterm window where you are logged in as root, type:  
`/usr/sbin/redhat-config-network`
2. In the tool window, select the appropriate network adapter (e.g. eth0).
3. Select Edit from the menu bar.
4. Select the "Automatically obtain IP Address Settings with DHCP" option.
5. Select the "Automatically obtain DNS Information from Provider" checkbox.
6. Click **Ok**.
7. Select **File > Save** from the menu bar.
8. Reboot the workstation.

### *Browser Requirements for Web-Based Authentication*

These instructions pertain to web-based authentication only. In order to launch the authentication web page, the end user must have access to one of the following supported web browsers.

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

## **Installing and Configuring the RADIUS Server**

Policy Manager has been designed to work with a RADIUS server for authentication. It exchanges information between a RADIUS client (a device that provides network access to users) and a RADIUS authentication server (a device that contains authentication information for these users).

There are many RADIUS server products available. Policy Manager has been tested with the following:

- FreeRADIUS
- Windows Server 2008 Network Policy Server
- Windows Server 2003 Internet Authentication Service
- Windows Server 2000 Internet Authentication Service
- Steel-Belted RADIUS

To give you an idea of how to configure your RADIUS server, we are providing instructions for configuring the RADIUS server using Funk's Steel Belted RADIUS Administrator user interface. If you are using another vendor's product, adapt the instructions as needed.

After installing your RADIUS server and user interface, you will need to use the user interface to configure your Policy Manager devices (RADIUS client devices) and end users on the server. The RADIUS server user interface is sometimes called the "client". This is not to be confused with the RADIUS client devices that you will be adding to the server.

---

**NOTES:** The procedures below may vary depending on the operating system you are using.

**Configuring Windows Server 2008**

Users of Windows Server 2008 should read this Authentication Configuration Guide, but should follow the steps in [Configuring a Windows Server 2008 for RADIUS Authentication](#) for instructions on installing and configuring the RADIUS server.

**Configuring Windows 2000 Advanced Server and Windows Server 2003**

Users of Windows 2000 Advanced Server and Windows Server 2003 should read this Authentication Configuration Guide, but should follow the steps in [Configuring a Windows Server 2000 or 2003 for RADIUS Authentication](#) for instructions on installing and configuring the RADIUS server.

**Configuring Windows 2000**

Windows 2000 users who plan to utilize Funk Software Inc.'s Steel-Belted RADIUS should consult Funk's website [www.funk.com](http://www.funk.com) for assistance in setting up Steel-Belted RADIUS on Windows 2000, in particular Tech Bulletins RD 410 and RD 447 (look for Tech Support > Steel-Belted Radius > Steel-Belted Radius Tech Notes > View by Tech Note ID Number).

---

### *Installing the RADIUS Server*

Install your RADIUS server and its user interface according to the vendor's instructions. In preparation, read the following installation requirements:



- The RADIUS server must be installed on a machine other than the one where Policy Manager is installed.
- Make sure you install the RADIUS server on a machine whose operating system is supported by the vendor's product.
- You'll need to install both the RADIUS server and the RADIUS user interface (or RADIUS client -- in Steel Belted RADIUS, it's called the Steel Belted RADIUS Administrator). However, they do not need to be on the same machine.
- Be sure to read the vendor's release notes prior to installing.
- Have on hand the license key provided to you by your vendor.
- You must be logged in as Administrator, or another user with full read/write privileges.

### *Adding RADIUS Client Devices*

Now that you've installed the RADIUS server and user interface, you will add the RADIUS clients (Policy Manager devices, not end users) to the server. If you are using a RADIUS server other than Funk Software Inc.'s Steel-Belted RADIUS, you will need to adapt the instructions below to your product.

1. From the Windows **Start** menu, select **Settings > Control Panel > Services** and confirm that the RADIUS server is running by scrolling down to Steel Belted Radius Server. The Status of the server should be "Started." If it is not running, start it by clicking **Start**.
2. Close the Services window.
3. Open the RADIUS server user interface (**Start > Programs > Steel Belted Radius > Steel Belted Radius Administrator**).
4. Click **Connect** to connect to the local RADIUS server.
5. Select **RAS Clients**.
6. Click **Add**.
7. **Client Name**: If the device has a name that can be resolved to an IP address, enter the name. Otherwise, enter its IP address.
8. **IP Address**: Enter the IP address of the device.
9. **Make/Model**: Verify that Standard Radius is selected.
10. Select **Edit authentication shared secret**.

11. **Shared Secret:** Enter a string of characters that will be used to encrypt and decrypt communications between the RADIUS server and the device (RADIUS client). Without the shared secret, the server and client will be unable to communicate, and authentication attempts will fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not. Be sure to write the shared secret down, as you will be adding it to the RADIUS client devices later.

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. N-Series devices with firmware version 5.0 or above, and S-Series devices are an exception to this, as these devices **do** support a unique shared secret for each server.

12. Click **Set**.

13. Repeat until all of your Policy Manager devices have been added.

### *Adding RADIUS Users*

In order for your end users to communicate with the RADIUS server, you need to add them to the RADIUS server and map them to the appropriate Policy Manager roles. You will do this with the RADIUS user interface. You can add RADIUS users as Native users (local users) or as Domain users (defined on a domain controller) or both.

**NOTE:** If you are configuring MAC authentication in addition to 802.1X and/or Web-based authentication, you will need to make two entries for each end user: one for the MAC address and one for the user name.

**NOTE:** For information on configuring end user VLAN ID attributes (in compliance with RFC 3580) to be used in conjunction with [VLAN to Role Mapping](#), refer to your device firmware and RADIUS server documentation.

**Preparation:** In order to add RADIUS users, you need to know what role names will apply to each user. See [Planning Your Policies](#) for more information.

### **Adding Native (Local) Users**

1. In the RADIUS client window (Steel Belted RADIUS Administrator window), select **Users**.
2. Click **Add**.
3. In the **Add New User** window, verify that the Native tab is selected.

4. In the **Enter User Name** field, enter the user name, and click **OK**.  
**NOTE:** If you are configuring MAC authentication, enter the MAC address in the Enter User Name field. When you enter the MAC addresses, do not use dots, semi-colons, or colons as delimiters. The correct format is as follows: `XX-XX-XX-XX-XX-XX`
5. Click **Set Password**.
6. In the **Enter User Password** window, enter the user's password.  
**NOTE:** If you are configuring MAC authentication, enter the MAC password in the Enter User Password field.
7. Click **Set**.
8. Select **Allow CHAP**. (You can also use PAP for native users. PAP would be used for users configured on a domain controller.)
9. Click **Set**.
10. In the **Users Window**, select the **Return list attributes** tab and click **Ins**.
11. **Add New Attributes** window: In the Available Attributes panel, click **Filter-Id**.
12. In the **Enter a String** field, enter:  
**Enterasys:version=1:mgmt=su:policy=[role]**  
where `[role]` is the role name to be applied to this user.

---

**CAUTION:** Include `:mgmt=su` in the string only for users who should have administrative privileges and the ability to telnet to devices and/or use local management on devices when authentication is enabled. For other users, leave it out.

---
13. Click **Add**, then **Close**, then **Save**.
14. Repeat until all of your native users have been added.

## Adding Domain Users

If you are going to add domain users, they must be set up in your Domain Controller first.

1. In the RADIUS client window (Steel Belted RADIUS Administrator window), select **Users**.
2. Click **Add**.
3. In the **Add New User** window, select the Domain tab.

4. Select a domain on the left pane and users or groups on the right pane, and click **OK**.
  5. Click **Ins**.
  6. **Add New Attributes** window: In the Available Attributes panel, click **Filter-Id**.
  7. In the **Enter a String** field, enter:  
**Enterasys:version=1:mgmt=su:policy=[role]**  
where `[role]` is the role name to be applied to this user.
- 
- CAUTION:** Include `:mgmt=su` in the string only for users who should have administrative privileges and the ability to telnet to devices and/or use local management on devices when authentication is enabled. For other users, leave it out.
- 
8. Click **Add**, then **Close**, then **Save**.
  9. Repeat until all of your domain users have been added.

## Configuring RADIUS in Policy Manager

Now that the RADIUS server side has been set up, you can complete your configuration using Policy Manager. The steps are as follows:

1. [Downloading the Firmware](#)
2. [Adding Devices to Policy Manager](#)
3. [Configuring the Port Mode](#)
4. [Configuring Devices as RADIUS Clients](#)
5. [Configuring Authentication on Devices](#)

### *Downloading the Firmware*

Policy Manager works with devices that support the Enterasys Policy Profile and Enterasys Web Authentication MIBs, such as the S-Series and K-Series devices. Follow the instructions that come with your hardware to download the latest authentication image (which includes the MIBs) to your devices. An easy way to download firmware to multiple devices is to use NetSight Inventory Manager, or you can use NetSight Console to download firmware to a single device.

Once you have downloaded the firmware, clear NVRAM on all the devices.

## *Adding Devices to Policy Manager*

Policy Manager and Console share the NetSight database which contains the device models that represent the actual devices in your network. There are three ways to add devices to the NetSight database. Initially, you must perform a Console Discover to populate the database or you can also use Console to import devices from a .ngf file. Once devices have been added to the NetSight database, you must assign the devices to a [Policy Domain](#) using Policy Manager. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy Manager Network Elements tree. Only devices assigned to the domain you are currently viewing are displayed.

After you have initially added your devices, you can use Policy Manager's Add Device window to add a single device to the database and the current domain. See [How to Add and Delete Devices](#) for information and instructions.

## *Configuring the Port Mode*

The [port mode](#) for the following port types should be set to Inactive/Default Role. This will prevent losing contact with your devices when authentication is enabled. Since this is the default port mode for all ports, you only need to confirm that these ports are set correctly.

- Router ports
- RADIUS server ports
- NetSight Policy Manager port
- DHCP/DNS/WINS server ports
- Backplane ports
- Front panel interswitch link ports

To confirm that the required ports are set to Inactive/Default Role:

1. Launch Policy Manager.
2. In the left panel, select the Network Elements tab.
3. Open the All Devices folder and select the device on which the port is located.
4. Select the right-panel Ports tab for the device and click **Retrieve**. Scroll to the right to see the Port Mode column and verify that the Port Mode for the port is Inactive/Default Role.

If the port mode for a port is incorrect, do the following:

1. Right click on the port and select Properties. The Port Properties window opens.
2. Select the Authentication Configuration tab.
3. Select the General sub-tab. In the Port Mode area, set the port as follows:  
**Authentication Behavior:** Inactive  
**Unauthenticated Behavior:** Default Role
4. Click **Apply**. To confirm that the port was set to Inactive/Default Role, select the right-panel Ports tab for the applicable device and check the Port Mode column for the port.

**NOTE:** The procedures above enable you to set a few ports quickly for testing purposes. If you need to set a large number of ports, you may want to use the [Port Configuration Wizard](#), which includes windows where you can set up authentication parameters and default roles and apply them to multiple ports. See the [How to Configure Ports](#) Help topic for more information.

### *Configuring Devices as RADIUS Clients*

You can now use Policy Manager to configure each device as a RADIUS client.

---

**CAUTION:** Be sure you have completed the previous task, [Configuring the Port Mode](#), before moving on to this procedure. Otherwise, you may lose contact with your devices.

---

Configure each device as follows (see the [RADIUS Tab](#) Help topic for more information):

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the RADIUS tab.
3. In the RADIUS Server(s) area, select the Authentication sub-tab and click **Add** to open the [Add RADIUS Authentication Server window](#).
4. Enter the following information:

**Authentication Server IP:** [IP address of your RADIUS server]  
**Authentication Client UDP Port:** 1812

---

**NOTE:** Depending on what RADIUS server you are using, another client UDP port might be appropriate. For example, 1645 is the client UDP port used by Funk Software, Inc.'s RADIUS™ version 2.25.80). 1812 is the client UDP port used by many other RADIUS servers.

---

**Server Shared Secret:** This must match the RADIUS server shared secret

entered when you [added the client device to the RADIUS server](#).

**Verify Shared Secret:** Retype the shared secret to confirm.

---

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above and Matrix S-Series devices are an exception to this, as these devices **do** support a unique shared secret for each server.

---

**Auth. Access Type:** Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- **Any access** - the server can authenticate users originating from any access type.
- **Management access** - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

This feature allows you to have one set of servers for authenticating management access requests and a different set for authenticating network access requests. Devices that do not support this feature will have this field grayed out.

**Server Priority:** Select the order in which the RADIUS authentication server will be checked, as compared to the other RADIUS authentication servers on the device. The lower the number, the higher the priority.

5. If this is the only RADIUS server you are adding, click **OK**. If you are adding another RADIUS server for backup or for another reason, click **Apply** and repeat steps 4 and 5.
6. On the RADIUS tab, click the **Apply** button in the RADIUS Server(s) section.
7. In the RADIUS Authentication Client Settings section, set the **RADIUS Client Status** field to Enabled, and click the **Apply** button in that section.

### *Configuring Authentication on Devices*

Now, use Policy Manager to configure authentication on each device. The steps you will use depend on the authentication type(s) you are configuring. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two

authentication types and single users per port (Single User Authentication). Refer to the NetSight Firmware Support tables for information on the authentication types supported by each device type.

Configure the appropriate authentication types as follows (see the Help topic [Authentication Tab \(Device\)](#) for more information).

---

**WARNING:** Leaving the default multi-user authentication type precedence is recommended. In particular, changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type can cause problems.

---

## Web-Based Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Single User Web-Based or Multi-User Web-Based  
**Authentication Status:** Enabled  
For devices that support multi-authentication types, you can set the **Multi-User Authentication Type Precedence**. This allows you to set the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.
3. Click the **Apply** button in the General Settings section.
4. In the Web Authentication Settings sub-tab, select the General sub-tab and select/enter the following information:  
**Enhanced Login Mode:** Enable this feature, if desired. (This option is grayed out if not supported on the device.)  
**Logo Display Status:** Select Show or Hide, as desired. (This option is grayed out if not supported on the device.)  
**WINS/DNS Spoofing:** Select Enabled. (This option is grayed out if not supported on the device.)  
**Authentication Protocol:** Select PAP  
**Web Authentication URL:** Enter the URL for your authentication web page. (This option is grayed out if not supported on the device.)  
**Web Authentication IP Address:** Enter the IP address of your authentication web page server.
5. Click the **Apply** button at the bottom of the tab.



6. Still in the Web Authentication Settings sub-tab, select the Web Login sub-tab and modify the Web Page Banner the end users will see at the top of the authentication web page so that it fits your needs. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful logon and failed authentication, as well as on the "Radius Busy" screen, it would not be appropriate to include "Welcome to [Your Company]" in the banner.
7. Click the **Apply** button at the bottom of the tab.
8. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

### 802.1X Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Single User 802.1X or Multi-User 802.1X  
**Authentication Status:** Enabled  
For devices that support multi-authentication types, you can set the **Multi-User Authentication Type Precedence**. This allows you to set the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.
3. Click the **Apply** button in the General Settings section.
4. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

### MAC Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Single User MAC or Multi-User MAC  
**Authentication Status:** Enabled  
For devices that support multi-authentication types, you can set the **Multi-User Authentication Type Precedence**. This allows you to set the order in

which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.

3. Click the **Apply** button in the General Settings section.
4. In the MAC Authentication Settings sub-tab, specify the MAC authentication password that will be used for that device.
5. Click the **Apply** button at the bottom of the tab.
6. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

### 802.1X+MAC Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Single User 802.1X+MAC  
**Authentication Status:** Enabled
3. Click the **Apply** button in the General Settings section.
4. In the MAC Authentication Settings sub-tab, specify the MAC authentication password that will be used for that device.
5. Click the **Apply** button at the bottom of the tab.
6. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

### CEP Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Single User CEP or Multi-User CEP  
**Authentication Status:** Enabled  
For devices that support multi-authentication types, you can set the **Multi-User Authentication Type Precedence**. This allows you to set the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be

tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.

3. Click the **Apply** button in the General Settings section.
4. In the CEP sub-tab, select the CEP product types supported on the device, and map a role for each type. Then, when a convergence endpoint (such as an IP phone) connects to the network, the device identifies the type of endpoint and applies the assigned role. Click **Add** to open the Add CEP Mapping window where you can select a CEP product type supported on the device, and map a role for that type. Click **OK**.
5. Click the **Apply** button at the bottom of the tab.
6. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

**NOTE:** In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access sub-tab in the [Port Properties Authentication Configuration Tab](#) or the [Port Configuration Wizard](#).

## Quarantine Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Multi-User Quarantine  
**Authentication Status:** Enabled
3. Click the **Apply** button in the General Settings section.
4. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

For more information on Quarantine Authentication requirements, see [How to Configure Quarantine Authentication](#).

## Auto Tracking Authentication

1. In the left-panel Network Elements tab, select the device.
2. In the right panel, select the [Authentication tab](#) and make the following selections in the General Settings section:  
**Authentication Type:** Multi-User Auto Tracking  
**Authentication Status:** Enabled

3. Click the **Apply** button in the General Settings section.
4. Repeat until all of your devices have been configured. If you are configuring multiple devices, you may want to use the [Device Configuration Wizard](#).

For more information on Auto Tracking Authentication requirements, see [How to Configure Auto Tracking Authentication](#).

## Testing Authentication

Upon completion of the steps in this document and any additional steps contained in the [Configuration Supplements](#) that are applicable to your authentication type, you will need to test your authentication configuration. This section provides two testing scenarios: one for web-based authentication and one for 802.1X authentication.

If your tests are successful, you can go on to create your remaining roles and services, referring to your plan and to the Help topics [How to Create a Role](#) and [How to Create a Service](#) as needed.

If your test is unsuccessful and you have issues you cannot resolve by reviewing the configuration steps in this document, contact Extreme Networks Support for assistance.

### *Testing Web-Based Authentication*

In order to test your web-based authentication configuration, you will use Policy Manager to create one of the roles from the plan you worked out earlier. You do not need to create the role's services and classification rules at this time; only the role name is required for the test.

After creating the role, you will enforce it (write it to the device). You will then configure the port mode on one port to be Active/Discard and another to be Active/Default Role. Finally, you will attempt to log in to both ports as one of the users you mapped to the role on the RADIUS server.

---

**NOTE:** Because Multi-User Web-Based Authentication does not support the Active/Discard port mode, you must configure your device with Single User Web-Based Authentication in order to perform the following Active/Discard mode test.

---

## Preparation

1. Decide on the role you want to test. It might be helpful to test the role that is assigned to your own user ID.
2. Create the role as follows:
  - a. In Policy Manager, select the Roles tab in the left panel.
  - b. Right-click the Roles folder, and select Create Role.
  - c. Type the role name in the highlighted box and press **Enter**.
  - d. Click **Enforce** on the toolbar, review the effects of enforcing on the [Enforce Preview window](#) if it is enabled, then click **Enforce** on that window. This writes the role to the devices, making them aware of the role's existence, but it does not associate the role with any port.
3. Select the Network Elements tab in the left panel.
4. Select a port to use as an Active/Discard mode port.
  - a. Select the right-panel Ports tab for the device where the port resides and click **Retrieve**.
  - b. Right click on the port and select Properties. The Port Properties window opens.
  - c. Select the Authentication Configuration tab.
  - d. Select the General sub-tab. In the Port Mode area, set the port as follows:  
**Authentication Behavior:** Active  
**Unauthenticated Behavior:** Discard
5. Select a port to use as an Active/Default Role mode port.
  - a. Right click on the port and select Properties. The Port Properties window opens.
  - b. Select the Authentication Configuration tab.
  - c. Select the General sub-tab. In the Port Mode area, set the port as follows:  
**Authentication Behavior:** Active  
**Unauthenticated Behavior:** Default Role
  - d. Assign a default role to the port by right-clicking the port and selecting Set Default Role.
  - e. Select the role you created earlier, and click **OK**. Now the role is associated with the port.

6. To confirm that the ports are set correctly, select the right-panel Ports tab for the device and view the Default Role and Port Mode columns for the ports you just configured.

### Testing Active/Discard Mode

---

**NOTE:** Because Multi-User Web-Based Authentication does not support the Active/Discard port mode, you must configure your device with Single User Web-Based Authentication in order to perform the following Active/Discard mode test.

---

Active/Discard mode means that authentication is enabled on the port, and unauthenticated traffic is not allowed. For this test, the Active/Discard mode port should behave as follows, as displayed on the [Ports tab](#) for the device:

- Prior to user login, the Default Role for the port is <None>, and the Current Role for the port is also <None>.
  - After successful login, the Default Role for the port is still <None>, but the Current Role for the port becomes the user's assigned role.
  - After the user logs out, the Default Role is still <None> and the Current Role reverts to <None>.
- 

**NOTE:** This test assumes the end user workstation is [configured as a DHCP client](#). If your end users use static IP addresses, they must be on the 192.168.0.0 network (with a mask of 255.255.0.0) or have a route to it. Otherwise, they will not be able to access the login screen for authentication.

---

To test your authentication configuration in Active/Discard mode:

1. Before the user is authenticated, verify that the Active/Discard port you configured earlier does not allow unauthenticated traffic to pass in either direction.
2. Configure a user machine to be a DHCP client and connect it to the Active/Discard port.
3. On the Ports tab, look at the Default Role and Current Role for the selected port. They should both be <None>.
4. On the user machine, confirm that you can get the correct IP address, as follows:

**Windows:** Open a DOS window and enter: **ipconfig /renew**

**Solaris:** At the prompt, enter: **ifconfig le0 dhcp**

The IP address should be 192.168.1.[port number] where [port number] is the port number on the device to which the user machine is

connected. End users who use DHCP receive this temporary IP address from the device. This IP address provides access to the authentication login web page. If authentication is successful, the user can obtain a permanent IP address from the DHCP server.

5. On the user machine, open your Firefox or Internet Explorer browser.
6. If you are using Netscape, disable the proxy (unless you have performed one of the other proxy configuration procedures in [Browser Requirements](#), earlier).
7. Bring up the authentication login web page URL that you entered in the Web Authentication section of the Authentication tab.
8. Type in the user name and password for the user being tested, and click **Login to Network**. Within a few seconds, you should see the message **Welcome to the Network**.

If the Welcome message does not appear, check the following:

- Make sure you entered the user name and password correctly in the RADIUS server.
- If the message "Access is Denied" appears, it could mean the device cannot reach the RADIUS server. Possible causes include:
  - The device's IP address has not been properly entered in the RADIUS server
  - The device has not been enabled as a RADIUS client
  - The RADIUS server has not been properly specified on the device
  - The correct client UDP port for the RADIUS server has not been specified in Policy Manager
- Other possible causes of the "Access is Denied" message include:
  - The wrong user/password combination was entered
  - The user is not in the database
  - The wrong authentication protocol has been specified (PAP vs. CHAP) on the device.
  - The wrong shared secret has been specified on the device

**NOTE:** In the event of errors, the RADIUS server log for today's date may assist in troubleshooting. For Funk RADIUS servers, this file is located in the Service directory in your RADIUS server installation area. For Microsoft Authentication servers, view this information in the Event Viewer.

9. To confirm that your authentication was successful, do the following:
  - To see that the role was assigned to the port, in Policy Manager, look at the Ports tab for the device again. The Default Role should say <None>, and the Current Role should be the one assigned to the user who just logged on.
  - To see that the user machine has the new IP address, issue the **ipconfig /all** (Windows) or **ifconfig le0 dhcp** (Solaris) command at the command prompt.
  - To see that the user is a client in the DHCP IP address scope, on the DHCP services machine open the DHCP Manager, double-click Local Machine, and double-click the scope. The Active Lease window opens to show you the active DHCP clients.
10. On the user machine, return to the web authentication URL and log off the network. To confirm that your role is no longer active on the port, return to the Policy Manager Ports tab for the device and note that the Current Role for the port again says <None>.
11. Verify again that the port does not allow unauthenticated traffic to pass in either direction.

### Testing Active/Default Role Mode

Active/Default Role mode means that authentication has been enabled on the port, but a default role will apply in the absence of an authenticated user. A user does not need to authenticate to access the (usually limited) services provided by the default role. However, a user may opt to authenticate in order to access the (possibly more robust) services provided by his or her own role. For this test, the Active/Default Role mode port should behave as follows, as displayed on the [Ports tab](#) for the device:

- Prior to user login, the Default Role for the port is whatever role has been assigned as the default in Policy Manager, and the Current Role is the same as the Default Role.
- After successful login, the Default Role remains the assigned default role for the port, but the Current Role becomes the user's role.
- After the user logs off, the Current Role reverts to the Default Role.

---

**NOTE:** This test assumes the user has a static IP address. End users who use static IP addresses must be on the 192.168.0.0 network (with a mask of 255.255.0.0) or have a route to it.

---

To test your authentication configuration in Active/Default Role mode:



1. Connect a user machine to the Active/Default Role port to which you assigned the default role earlier.
2. In Policy Manager, on the Ports tab for the device, confirm that the Default Role and Current Role for that port are identical.
3. On the user machine, bring up the authentication login web page URL that you entered in the Web Authentication section of the Authentication tab.
4. Type in the user name and password, and click **Login to Network**. Within a few seconds, you should see the message **Welcome to the Network**. If the Welcome message does not appear, refer to the suggestions under [step 8](#) in the previous section.
5. In Policy Manager, look at the Ports tab for the device again. The Default Role should be the role you assigned as the default for the port, but the Current Role should be the one assigned to the user who just logged on.
6. On the user machine, return to the web authentication login page and log off the network. To confirm that the role for the port has reverted to the default, return to the Policy Manager Ports tab for the device and note that the Current Role for the port is again the same as the Default Role.

### *Testing 802.1X Authentication*

In order to test your 802.1X authentication configuration, you will use Policy Manager to create one of the roles from the plan you worked out earlier. You do not need to create the role's services and classification rules at this time; only the role name is required for the test.

After creating the role, you will enforce it (write it to the device). You will then configure the port mode on one port to be Active/Discard and another to be Active/Default Role. Finally, you will attempt to log in to both ports as one of the users you mapped to the role on the RADIUS server.

---

**NOTE:** Be sure to complete the additional configuration steps in the [802.1X Authentication Configuration Supplement](#) prior to performing this test.

---

### Preparation

1. Decide on the role you want to test. It might be helpful to test the role that is assigned to your own user ID.

2. Create the role as follows:
  - a. In Policy Manager, select the Roles tab in the left panel.
  - b. Right-click the Roles folder, and select Create Role.
  - c. Type the role name in the highlighted box and press **Enter**.
  - d. Click **Enforce** on the toolbar, review the effects of enforcing on the [Enforce Preview window](#) if it is enabled, then click **Enforce** on that window. This writes the role to the devices, making them aware of the role's existence, but it does not associate the role with any port.
3. Select the Network Elements tab in the left panel.
4. Select a port to use as an Active/Discard mode port.
  - a. Select the right-panel Ports tab for the device where the port resides and click **Retrieve**.
  - b. Right click on the port and select Properties. The Port Properties window opens.
  - c. Select the Authentication Configuration Settings tab.
  - d. Select the General sub-tab. In the Port Mode area, set the port as follows:  
**Authentication Behavior:** Active  
**Unauthenticated Behavior:** Discard
  - e. If you have configured Single User 802.1X or 802.1X+MAC authentication types, Active/Discard mode requires that any default role set on the port is cleared. If you have set a default role for this port, you will be prompted to clear it.
5. Select a port to use as an Active/Default Role mode port.
  - a. Right click on the port and select Properties. The Port Properties window opens.
  - b. Select the Authentication Configuration Settings tab.
  - c. Select the General sub-tab. In the Port Mode area, set the port as follows:  
**Authentication Behavior:** Active  
**Unauthenticated Behavior:** Default Role
  - d. If you have configured Single User 802.1X or 802.1X+MAC authentication types, Active/Default Role mode requires that you set a default role on the port, and you will be prompted to assign a role.

Otherwise, you must assign a default role to the port by right-clicking the port and selecting Set Default Role.

- e. Select the role you created earlier, and click **OK**. Now the role is associated with the port.
6. To confirm that the ports are set correctly, select the right-panel Ports tab for the device and view the Default Role and Port Mode columns for the ports you just configured.

### Testing Active/Discard Mode

Active/Discard mode means that authentication is enabled on the port, and unauthenticated traffic is not allowed. For this test, the Active/Discard mode port should behave as follows, as displayed on the [Ports tab](#) for the device:

- Prior to user login, the Default Role for the port is <None>, and the Current Role for the port is also <None>.
- After successful login, the Default Role for the port is still <None>, but the Current Role for the port becomes the user's assigned role.
- After the user logs off, the Default Role is still <None> and the Current Role reverts to <None>.

To test your authentication configuration in Active/Discard mode:

1. Before the user is authenticated, verify that the Active/Discard mode port you configured earlier does not allow unauthenticated traffic to pass in either direction.
2. Connect a user machine to the port.
3. On the Ports tab, look at the Default Role and Current Role for the selected port. They should both be <None>.
4. On the user machine, log on to the network.
5. In Policy Manager, look at the Ports tab for the device again. The Default Role should be <None>, but the Current Role should be the one assigned to the user who just logged on.
6. On the user machine, log off the network. To confirm that your role is no longer active on the port, return to the Ports tab for the device and note that the Current Role for the port again says <None>.
7. Verify again that the port does not allow unauthenticated traffic to pass in either direction.

## Testing Active/Default Mode

Active/Default Role mode means that authentication has been enabled on the port, but a default role will apply in the absence of an authenticated user. A user does not need to authenticate to access the (usually limited) services provided by the default role. However, a user may opt to authenticate in order to access the (possibly more robust) services provided by his or her own role. For this test, the Active/Default Role mode port should behave as follows, as displayed on the [Ports tab](#) for the device:

- Prior to user login, the Default Role for the port is whatever role has been assigned as the default in Policy Manager, and the Current Role is the same as the Default Role.
- After successful login, the Default Role remains the assigned default role for the port, but the Current Role becomes the user's role.
- After the user logs off, the Current Role reverts to the Default Role.

To test your authentication configuration in Active/Default Role mode:

1. Connect a user machine to the Active/Default Role mode port to which you assigned the default role earlier.
2. In Policy Manager, on the Ports tab for the device, confirm that the Default Role and Current Role for that port are identical.
3. On the user machine, log on to the network.
4. In Policy Manager, look at the Ports tab for the device again. The Default Role should be the role you assigned as the default for the port, but the Current Role should be the one assigned to the user who just logged on.
5. On the user machine, log off the network. To confirm that the role for the port has reverted to the default, return to the Policy Manager Ports tab for the device and note that the Current Role for the port is again the same as the Default Role.

---

## Related Information

For information on related concepts:

- [Authentication](#)
- [Policy Manager Concepts](#)
- [Traffic Classification Rules](#)

For information on related tasks:

- [Getting Started with Policy Manager](#)
- [How to Configure Devices](#)
- [How to Configure Ports](#)
- [How to Create a Role](#)
- [How to Create a Service](#)
- [How to Create or Modify a Rule](#)

For information on related windows:

- [Authentication Tab \(Device\)](#)
- [RADIUS Tab \(Device\)](#)
- [Add RADIUS Authentication Server Window](#)
- [Add RADIUS Accounting Server Window](#)

## How to Configure Auto Tracking Authentication

---

Auto tracking is a form of authentication that is used to track session information for traffic that is not authenticated by the other supported authentication types (802.1x, PWA, MAC, CEP, and Quarantine). With auto tracking enabled, these sessions are entered into the session table, allowing network administrators to determine which end-systems on which ports are not being authenticated through traditional authentication methods.

When an end-system connects and does not authenticate using any of the other authentication methods, an auto tracking session is created. The end-system is assigned the appropriate policy as configured in Policy Manager, such as the port's default role.

Auto tracking provides the administrator with increased visibility into who is on the network and where. Because these sessions are tracked, an administrator can determine whether and how to provision them in the future, allowing for increased security and control.

There are two main steps to configuring auto tracking authentication:

- [Enable auto tracking authentication](#) on the device and port.
- [Set session properties](#) on the device and port.

---

**CAUTION:** Auto tracking authentication should not be used in domains that use MAC to role mappings or IP to role mappings that are based on destination MAC or IP addresses. For more information, see [Auto Tracking and Destination Role Mappings Compatibility](#).

---

## Enable Auto Tracking Authentication

Use the following steps to enable auto tracking authentication on the device and port. These instructions use the Device Authentication tab and Port Properties window. However, if you are configuring multiple devices and ports, you can use the [Device Configuration Wizard](#) and the [Port Configuration Wizard](#).

On the device:

1. Select the device in the left-panel Network Elements tab.
2. Select the right-panel [Authentication tab](#).

3. In the General Settings section, under Multi-User Authentication type, select the Auto Tracking checkbox.
4. Set Authentication Status to Enabled.
5. Click **Apply**.

**On the port:**

1. Select the device in the left-panel Network Elements tab.
2. In the right-panel Ports tab, select a port and click the Port Properties button.
3. In the Port Properties window, select the [Authentication Configuration tab](#) (in the top row of tabs).
4. Select the [General tab](#) (in the lower row of tabs).
5. Verify that the Port Mode Authentication Behavior is set to Active.
6. Verify that the Disable Auto Tracking Authentication for this port checkbox is not selected.
7. If you made any changes, click **Apply**.

## Set Session Properties

Use the following steps to configure session timeout and user count values on the device and port. These instructions use the Device Authentication tab and Port Properties window.

**On the device:**

1. Select the device in the left-panel Network Elements tab.
2. Select the right-panel Authentication tab.
3. Select the [Global Authentication Settings subtab](#).
4. Set the [session timeout](#) and [session idle timeout](#) values for Auto Tracking authentication.
5. Click **Apply**.

**On the port:**

1. Select the device in the left-panel Network Elements tab.
2. In the right-panel Ports tab, select a port and click the Port Properties button.

3. In the Port Properties window, select the [Authentication Configuration tab](#) (in the top row of tabs).
  4. Select the [Login Settings tab](#) (in the lower row of tabs).
  5. Set the [session timeout](#) and [session idle timeout](#) values for Auto Tracking authentication.
  6. Click **Apply**.
  7. Select the [Authenticated User Counts tab](#) (in the lower row of tabs).
  8. Set the [user count](#) value for Auto Tracking authentication.
  9. Click **Apply**.
- 

### Related Information

For information on related tasks:

- [Port Properties - Authentication Configuration Tab](#)
- [Device Authentication Tab](#)

## Auto Tracking and Destination Role Mappings Compatibility

Auto tracking authentication should not be used in domains that use MAC to role mappings or IP to role mappings that are based on destination MAC or IP addresses. (Source address mappings do not have the same compatibility concerns.) To understand the compatibility problem, consider how role mappings and auto tracking work.

Role mappings cause all traffic bound to the destination MAC or IP addresses to be processed by the role specified in the mapping, even though the traffic is originating from a user that may be assigned a different role via authentication or the port default. Traffic sent from the user to those destinations will be processed by the role defined in the mapping. Traffic sent from the user that is not to those destinations will continue to be processed by the role that user is authenticated to or assigned via the port default.

When auto tracking is enabled, auto tracking authentication sessions are created for all traffic detected on enabled ports. If a user is assigned a role by another authentication type there will be no compatibility issue because the auto tracking authentication precedence is lower than all other authentication types. However, if a user is assigned the port default role (which has a lower



precedence than all authentication types including auto tracking), and the first traffic from the user happens to be to one of the mapped destination addresses, then an auto tracking authentication session will be created with the role specified by the mapping rather than the port default role. This will cause all traffic from that user to be processed by the mapping role. Since this is not likely to be the same role as specified by the port defaults, the user may not have traffic classified in the manner expected.

---

### **Related Information**

For information on related tasks:

- [How to Configure Auto Tracking Authentication](#)

# 802.1X Authentication Configuration Supplement

---

This Help topic provides supplemental instructions for users who are configuring their network for 802.1X authentication. It is recommended that you begin by following the instructions in the Policy Manager [Authentication Configuration Guide](#). Then, read this configuration supplement for specific information related to configuring 802.1X end users. For more detailed information regarding client setup, consult the documentation for your particular client(s).

Instructions on:

- [EAP MD5-Challenge End User \(Supplicant\) Setup](#)
  - [Windows XP and Windows 2000 End User \(Supplicant\) Setup](#)
    - [How to Speed up MD5 Prompt on XP Client](#)
  - [Linux SecureSupplicant Setup](#)
- [EAP-TLS Certificate Setup](#)
  - [Windows 2000 AS Certificate Server Configuration](#)
  - [Windows XP Client Certificate Setup](#)
- [802.11 Wireless Setup](#)
  - [RoamAbout R2 802.1X Configuration](#)

## EAP MD5-Challenge End User (Supplicant) Setup

### *Windows XP and Windows 2000 End User (Supplicant) Setup*

Use the following instructions to set up a Windows XP or Windows 2000 end user for 802.1X authentication:

1. On the end user's machine, open Network Connections (Start menu > Settings > Network Connections).
2. Right click on the connection and select Properties.
3. In the General tab, verify that the **Show icon in notification area when connected** option is selected.
4. In the Authentication tab, select the **Enable network access control using**

IEEE 802.1X check box. Then, select **MD5-Challenge** as EAP type.

---

**NOTE:** Depending on your network's needs, you can select "Authenticate as computer when computer information is available" and/or "Authenticate as guest when user or computer information is unavailable".

---

The authentication process is as follows:

1. Press Ctrl-Alt-Delete and log on to the end user's machine.
2. Allow a couple of minutes (or less) to initialize and establish the EAP authentication between the local machine and the 802.1X-enabled device.
3. After establishing the EAP authentication, notice that a bubble (balloon) appears in the notification area.
4. Click on the bubble to open the network logon window.
5. Provide the end user's username and password, and the domain, if appropriate.

---

**NOTES:** If a user logs in incorrectly twice, the Windows XP client will not let them retry the login again. To be able to retry the login, the user can toggle link on the port, or log out and log back in.

After launching the network logon window by clicking the bubble, the user might get another bubble in the notification area before logging in. In this case, the user must close the logon window opened previously and click the second bubble which appeared in the notification area to re-launch the network logon window.

---

### How to Speed up MD5 Prompt on XP Client

By default, the MD5 prompt can take up to two minutes to appear after you log into the machine or plug into an 802.1X enabled device. It is possible to speed up this process by making the following changes to the XP client and the 802.1X-enabled device.

Modify the XP client's Registry:

1. Run regedit.exe from the Run box.
2. Navigate to HEY\_  
LocalMachine\Software\Microsoft\EAPOL\Parameters\General\Global.
3. Right click on Global and select **New** and the **DWORD** value.

4. Name it SupplicantMode.
5. After it is created, double-click it and set its value to a 3.
6. You must reboot the PC before the new registry value takes effect.

On the 802.1X-enabled device, use Policy Manager to change the Authentication Request Period on the supplicant port to a shorter interval:

1. Launch Policy Manager.
2. In the left panel, select the Network Elements tab.
3. Open the Devices folder and select the 802.1X-enabled device on which the port is located.
4. Select the port in the left panel.
5. In the right panel, select the Authentication Configuration tab.
6. In the Login Settings area, set the Authentication Request Period to a short interval, for example, 5 seconds.
7. Click **Apply**.

### *Linux SecureSupplicant Setup*

You can download the OpenSource 802.1X client from <http://www.open1x.org> at no cost, or you can purchase the Meetinghouse 802.1X supplicant called AEGIS Client from <http://www.mtghouse.com>. Refer to the instructions included in the download to install and set up your Linux SecureSupplicant.

## **EAP-TLS Certificate Setup**

### *Windows 2000 AS Certificate Server Configuration*

Use the following instructions to set up Windows 2000 Advanced Server (AS) for Certificate Authentication (CA). These instructions are only an example; refer to Microsoft documentation to install on a production network.

1. Install Windows 2000 Advanced Server with Active Directory, DNS service, and IAS.
2. If you did not install Internet Information Services (IIS) with the Windows 2000 AS installation, do so now.
  - a. Select the Start menu > Settings > Control Panel, and click on Add/Remove Programs.

- b. On the left panel, select Add/Remove Windows Components.
  - c. When the Windows Components window opens, select Internet Information Services (IIS), and Next. This will install the IIS service. You can now install the Certificate Services.
3. Launch the Windows Components Wizard by opening Add/Remove Programs in Control Panel and clicking on Add/Remove Windows Components.
4. When the Wizard opens, select Certificate Services from the component list. The installer will warn you that once the CA software is installed, you can't change the name of the server or move it out of an Active Directory Domain.
5. The Certification Authority Type Selection screen will appear, giving you a choice of the different CA types. Select Enterprise root CA. Do not select Advanced Options.
6. On the CA Identifying Information screen, enter a unique name for the CA Name, then fill out the rest of the form with whatever applies to your setup environment.
7. The next screen prompts you for the location of the Data Storage files. Select the defaults.
8. If you are running IIS WWW service, the installer will tell you that it must stop the service to complete the installation.
9. When the wizard finishes, you'll be prompted to restart your server. After rebooting, the CA service will start automatically.

### *Windows XP Client Certificate Setup*

Install a certificate on a Windows XP client:

1. Connect the client PC to the Domain on which the CA resides.
2. Open your browser and go to `http://<CA server>/certsrv`. This brings up the Certificate Services page for the CA server.
3. Select Request a Certificate.
4. Select User Certificate.
5. Select Submit. This prompts the client to request a certificate from the CA.
6. When the "Certificate Issued" response is presented, select "Install this Certificate". This results in "Certificate Installed".

View the installed certificate on the client:

1. Select the Start menu > Run.
2. Type `mmc`.
3. When the Console starts, select File > Add/Remove Snap-in.
4. From the Standalone tab, select **Add**.
5. Select Certificates, then **Add**.
6. The Certificates Snap-in window prompts for what type of account the certificate will manage.
7. Select **My user account**, then **Finish**.
8. Close the Add Standalone Snap-in window.
9. On the Add/Remove Snap-in window, click **OK**.
10. In the Console, expand Certificates, expand Personal, and select Certificates.
11. You will see your certificate(s) in the right pane.
12. Double-click on the certificate to view the certificate properties.
13. Upon initial authentication (within a few minutes of attempting), the client will be prompted to accept certificate as valid from server.

## 802.11 Wireless Setup

### *RoamAbout R2 802.1X Configuration*

Use the following instructions to set up and configure 802.1X authentication for the RoamAbout R2.

RoamAbout R2 firmware and boot images should be upgraded to the latest versions, which are available at <https://extranet.extremenetworks.com/downloads/Pages/RoamAbout4102.aspx>.

System requirements:

- RoamAbout R2 with RoamAbout card
- PC with Windows XP or Windows 2000 installed
- A null modem cable to connect the console port on the PC to the console port of the RoamAbout R2. (See <http://www.lammertbies.nl/comm/cable/RS-232.html#null>.)
- AP Manager installed on the PC

- A RADIUS Server with 802.1X support (Steel-Belted RADIUS Administrator Service Provider Edition) or Windows 2000 IAS

Configure the RoamAbout R2:

1. Connect a null modem cable from the PC to the RoamAbout R2.
2. Using a terminal emulator like Microsoft® HyperTerminal, log in to the RoamAbout R2.
3. Select Network Configuration, assign an IP mask and gateway, and save the configuration.
4. On the PC, launch AP Manager.
5. In AP Manager, select the **Add** button to add a new AP.
6. Upgrade the RoamAbout boot image to the latest version. To download the boot image:
  - a. In the AP Manager Main menu select **Reload**. The Reload window opens.
  - b. In the Options area, select the **Use This Computer** option.
  - c. In the Firmware Image area, select the **Operational BootROM** option.
  - d. Enter the path to the boot image or use the **Browse** button to navigate to the boot image.
  - e. Click **Reload Now**.
7. Upgrade the RoamAbout firmware image to the latest version. To download the firmware image:
  - a. In the Main menu select **Reload**.
  - b. In the Options area, select the **Use This Computer** option.
  - c. In the Firmware Image area, select the **Operational Firmware** option.
  - d. Enter the path to the firmware image or use the **Browse** button to navigate to the firmware image.
  - e. Click **Reload Now**.
8. When the images have finished downloading, at the prompt, reboot the RoamAbout R2 device.
9. In the AP Manager Main menu, select **Wireless Parameters**.
10. In the Wireless Parameters window, enter the Wireless Network Name.
11. Use Policy Manager to configure the RoamAbout R2 as a RADIUS client, following the instructions in the [Authentication Configuration Guide](#).

12. On the RoamAbout R2, you must enable 802.1X on each port by setting the port's Authentication Behavior to Active.
  - a. In Policy Manager, select the Network Elements tab in the left panel.
  - b. Expand the RoamAbout R2 device to see its ports.
  - c. Select a port in the left panel.
  - d. In the right panel, select the Authentication Configuration tab.
  - e. In the Port Mode area, set the port's Authentication Behavior to Active.
  - f. Click **Apply**.

Set up the Windows XP Client:

Requirements:

- A PC that meets windows XP requirements.
  - A wireless interface card on the XP PC.
1. Select Start menu > Settings > Network Connections and then right-click on wireless adapter icon.
  2. From the drop-down menu select Properties.
  3. Select the Authentication tab, and check **Enable network access control using the IEEE 802.1X**.
  4. Set EAP type to MD5 Challenge.

Set up the Funk RADIUS Server:

Requirements:

- RADIUS Server with 802.1X support (Steel-Belted RADIUS Administrator Service Provider Edition)
1. Install application.
  2. Go to the `eap.ini` file in in the RADIUS Services folder, and uncomment the `EAP-Type = MD5-Challenge` for the native, domain, and domain user groups.
  3. Go to the `RADIUS.ini` file and set the `LogLevel = 2` and the `TraceLevel = 2`. This sets logfile verbose level.
  4. Start RADIUS Server Service.



## Related Information

For information on related concepts:

- [Authentication](#)

For information on related tasks:

- [Authentication Configuration Guide](#)

## How to Configure Quarantine Authentication

---

Quarantine authentication allows you to assign a Quarantine role to an authenticated end user, thereby limiting or denying their ability to access the network. If an end user's traffic appears to be malicious, this enables you to quarantine the end user until further action can be taken.

Quarantine authentication works in conjunction with quarantine policy rules that assign a Quarantine role to the end user as part of their rule actions. When an end user authenticates to the network and is assigned a role, if their traffic matches a quarantine rule, they will be assigned a Quarantine role. The Quarantine role then restricts or prevents additional traffic from that user from entering the network, according to how the role is configured.

For example, let's say an authenticated end user is acting as a rogue DNS server on the network. Since a DNS server maps hostnames to IP addresses, this would allow them to direct traffic somewhere other than the legitimate destination. If the role assigned to the end user includes a quarantine rule that denies DNS traffic, the end user's traffic would be dropped and they would be assigned a Quarantine role to restrict or stop their access to the network. The end user will have to contact the administrator to regain access to the network.

There are four main steps to configuring quarantine authentication:

- [Define the Quarantine role](#).
- [Create a quarantine rule](#) that specifies the Quarantine role.
- [Enable quarantine authentication](#) on the device and port.
- [Set session properties](#) on the device and port.

### Define the Quarantine Role

With quarantine authentication, a Quarantine role is assigned to an end user to prevent or restrict their network access. You must define which of your roles will be used as the Quarantine role.

The Policy Manager default domain includes a Quarantine role that is configured to block all traffic. This default Quarantine role is used in conjunction with the Extreme Networks Intrusion Prevention System (IPS) and the NetSight Automated Security Manager to create an automatic response to threats detected on the network. In addition, the Quarantine role can be used by the

NetSight NAC Manager assessment functionality. Typically, you will want to use the default Quarantine role for quarantine authentication. If you make any changes to the Quarantine role, keep in mind that the role may be used by other applications and should remain highly restrictive in nature.

You can also create additional roles to use as Quarantine roles, if desired. Each role could have different restrictive behaviors, for example, you could create a role that allows limited internet access. Once you have created these roles, you can select them as the Quarantine role in your rules, just as you would the default Quarantine role. For information on creating a new role, see [How to Create a Role](#).

### Create a Quarantine Rule

Quarantine policy rules assign a Quarantine role to the end user as part of their rule actions.

Create a Quarantine rule using the classification rule type that identifies the traffic that you want to restrict from your network. Make sure that in the rule's actions you specify the Quarantine role to assign to the end user. When you have finished the rule, assign the service that includes the rule to your network roles and enforce.

For information on creating a rule, see [How to Create a Rule](#).

### Enable Quarantine Authentication

Use the following steps to enable quarantine authentication on the device and port. These instructions use the Device Authentication tab and Port Properties window. However, if you are configuring multiple devices and ports, you can use the [Device Configuration Wizard](#) and the [Port Configuration Wizard](#).

#### On the device:

1. Select the device in the left-panel Network Elements tab.
2. Select the right-panel [Authentication tab](#).
3. In the General Settings section, under Multi-User Authentication type, select the Quarantine checkbox.
4. Set Authentication Status to Enabled.
5. Click **Apply**.

#### On the port:

1. Select the device in the left-panel Network Elements tab.
2. In the right-panel Ports tab, select a port and click the Port Properties button.
3. In the Port Properties window, select the [Authentication Configuration tab](#) (in the top row of tabs).
4. Select the [General tab](#) (in the lower row of tabs).
5. Verify that the Port Mode Authentication Behavior is set to Active.
6. Verify that the Disable Quarantine Authentication for this port checkbox is not selected.
7. If you made any changes, click **Apply**.

## Set Session Properties

Use the following steps to configure session timeout and user count values on the device and port. These instructions use the Device Authentication tab and Port Properties window.

### On the device:

1. Select the device in the left-panel Network Elements tab.
2. Select the right-panel Authentication tab.
3. Select the [Global Authentication Settings subtab](#).
4. Set the [session timeout](#) and [session idle timeout](#) values for Quarantine authentication.
5. Click **Apply**.

### On the port:

1. Select the device in the left-panel Network Elements tab.
2. In the right-panel Ports tab, select a port and click the Port Properties button.
3. In the Port Properties window, select the [Authentication Configuration tab](#) (in the top row of tabs).
4. Select the [Login Settings tab](#) (in the lower row of tabs).
5. Set the [session timeout](#) and [session idle timeout](#) values for Quarantine authentication.
6. Click **Apply**.

7. Select the [Authenticated User Counts tab](#) (in the lower row of tabs).
  8. Set the [user count](#) value for Quarantine authentication.
  9. Click **Apply**.
- 

### **Related Information**

For information on related tasks:

- [How to Create a Role](#)
- [How to Create a Rule](#)

# Configuring a Windows Server 2008 for RADIUS Authentication

---

This Help topic provides instructions for users who wish to configure a Windows Server 2008 to provide RADIUS authentication. It includes steps for configuring Network Policy Server (NPS), and for creating users in Active Directory. Policy Manager has been designed to work with a RADIUS server for authentication. The NPS implements the RADIUS protocol, and provides authentication of users connecting to the network via LAN, virtual private network (VPN), and dial-up technology.

It is recommended that you begin by reading the Policy Manager [Authentication Configuration Guide](#) for general authentication instructions prior to following the steps here. Windows Server 2008 users should follow the steps in this topic, instead of the Installing and Configuring the RADIUS Server section in the Authentication Configuration Guide.

The recommended sequence for performing the configuration is listed below. When you have completed these instructions, refer back to the sections [Configuring RADIUS in Policy Manager](#) and [Testing Authentication](#) in the Authentication Configuration Guide for instructions on how to use Policy Manager to configure authentication parameters on your devices, and verify that the users created in Active Directory can authenticate to the network.

For more information on Windows Server 2008, access the [Microsoft Windows Server 2008 Step-by-Step Guides](#) and review the Windows Server 2008 Network Policy Server (NPS) Operations Guide.

---

**NOTE:** The following instructions assume that you already have NPS installed on your computer.

---

Instructions on:

1. [Configuring Network Policy Server \(NPS\)](#)
  - a. [Specifying RADIUS Port Numbers](#)
  - b. [Adding RADIUS Client Devices](#)
  - c. [Adding a New Remote Access Policy](#)

- d. [Registering NPS](#)
- e. [Stopping and Restarting NPS](#)
2. [Creating Users in Active Directory](#)
  - a. [Creating a User](#)
  - b. [Specifying User Permissions](#)
3. [Configuring Devices and Testing Authentication](#)

## Configuring Network Policy Server (NPS)

### *Specifying RADIUS Port Numbers*

Use the following steps to specify the RADIUS authentication and accounting port numbers.

1. Select **Start > Programs > Administrative Tools > Network Policy Server**. The Network Policy Server window opens.
2. Right click on "NPS (Local)" and select **Properties**.
3. In the Ports Tab, set the ports according to your RADIUS requirements.
4. Click **OK**.

### *Adding RADIUS Client Devices*

Follow these steps to add RADIUS clients (Policy Manager devices, not end users) to the server.

1. In the Network Policy Server window (Start > Programs > Administrative Tools > Network Policy Server), expand the RADIUS Clients and Servers folder.
2. Right-click on "RADIUS Clients" and select **New RADIUS Client**.
3. In the New RADIUS Client window, enter a Friendly name.
4. Enter the IP address of the RADIUS client and select a Client Vendor (e.g. RADIUS Standard).
5. Enter a Shared Secret. A shared secret is a string of characters that will be used to encrypt and decrypt communications between the RADIUS server and the device (RADIUS client). Without the shared secret, the server and client will be unable to communicate, and authentication attempts will fail. The shared secret must be at least 6 characters long; 16 characters is

recommended. Dashes are allowed in the string, but spaces are not. Be sure to write the shared secret down, as you will be adding it to the RADIUS client devices later.

6. Click **OK**.
7. Repeat until all of your Policy Manager devices have been added.

### *Adding a New Remote Access Policy*

Follow these steps to add a new Remote Access Policy. A Remote Access Policy is a set of actions which is applied to a group of users that meet a specified set of conditions. The selections in the following steps can be used as an example; for more specific options, review the [Windows Server 2008 Network Policy Server \(NPS\) Operations Guide](#).

---

**NOTE:** For information on configuring end user VLAN ID attributes (in compliance with RFC 3580) to be used in conjunction with [VLAN to Role Mapping](#), refer to your device firmware and RADIUS server documentation.

---

1. In the Network Policy Server window (Start > Programs > Administrative Tools > Network Policy Server), expand the Policies node. Right click on "Connection Request Policies" and select **New**.
2. The New Connection Request Policy wizard opens.
  - a. Enter a Policy name and then click **Next**.
  - b. In the Specify Conditions panel click **Add**.
  - c. Select the condition "Day and Time Restrictions" and click **Add**.
  - d. In the Day and Time Restrictions window select the **Permitted** radio button. Click **OK**. Click **Next**.
  - e. In the Specify Connection Request Forwarding panel, select "Authentication." Select the appropriate settings for your RADIUS server and click **Next**.
  - f. In the Specify Authentication Methods panel, click **Next**.
  - g. In the Configure Settings panel, click **Next**.
  - h. In the Completing Connection Request Policy Wizard panel, verify that the settings are correct and click **Finish**.
3. Back in the Network Policy Server window, right-click on "Network Policy" and select **New**.
4. The New Network Policy wizard opens.



- a. Enter a Policy name and click **Next**.
  - b. In the Specify Conditions panel, click **Add**.
  - c. Select the condition "Window Groups" and click **Add**.
  - d. In the Windows Groups window click **Add Groups**.
  - e. In the Select Group window, enter the object name to select. Click **OK**.
  - f. Click **OK** in the Window Groups window. Click **Next**.
  - g. In the Specify Access Permission Panel, select "Access Granted" and click **Next**.
  - h. In the Configure Authentication Methods panel, select the appropriate settings for your authentication requirements and click **Next**.
  - i. In the Configure Constraints panel, click **Next**.
  - j. In the Configure Settings panel, select "RADIUS Attributes Standard" and remove all parameters, such as "Server-Type" and "Framed-Protocol."
  - k. Click **Add** to add a Filter-Id attribute.
    - l. In the Add Standard RADIUS Attribute window, select "Filter-Id" and then click **Add**.
  - m. In the Attribute Information window, click **Add**.
  - n. In the Attribute Information window, enter the attribute value:  
**Enterasys:version=1:mgmt=su:policy=[role]**  
where [role] is the role name to be applied to this user.
- 
- CAUTION:** Include :mgmt=su in the string only for users who should have administrative privileges and the ability to telnet to devices and/or use local management on devices when authentication is enabled. For other users, leave it out.
- 
- o. Click **OK** and **Close** to close the windows and click **Next**.
  - p. In the Completing New Network Policy window, verify the settings are correct and click **Finish**.

### *Registering NPS*

Follow these steps to register the Network Policy Server in the Active Directory, which enables NPS to authenticate users in the Active Directory.

1. In the Network Policy Server window (Start > Programs > Administrative Tools > Network Policy Server), right click on "NPS (Local)" and select **Register server in Active Directory**.
2. Click **OK**.

### *Stopping and Restarting NPS*

After completing the above steps to configure the Network Policy Server, you must stop and restart the service.

1. In the Network Policy Server window (Start > Programs > Administrative Tools > Network Policy Server), right click on "NPS (Local)" and select **Stop NPS Service**.
2. Right click on "NPS (Local)" and select **Start NPS Service**.

## **Creating Users in Active Directory**

Use these steps to create users and specify user permissions.

### *Creating a User*

Create a new object for each user who will be authenticating.

1. Select **Start > Programs > Administrative Tools > Active Directory Users and Computers**. The Active Directory Users and Computers window opens.
2. Right click on the "Users" folder and select **New > User**.
3. Proceed through the windows, entering the user name, password, and other relevant information. Click **Finish**.

### *Specifying User Permissions*

For Windows Server 2008, user permission is specified in the [Remote Access Policy](#) that is configured in the Network Policy Server.

1. Right click on a user and select **Properties**. The User Properties window opens.
2. In the Dial-In tab, select the "Control access through NPS Network Policy" radio button in the Network Access Permission section.
3. Click **OK**.

## Configuring Devices and Testing Authentication

When you have completed the above instructions, refer to the sections [Configuring RADIUS in Policy Manager](#) and [Testing Authentication](#) in the Authentication Configuration Guide for instructions on how to use Policy Manager to configure authentication parameters on your devices, and verify that the users created in Active Directory can authenticate to the network.

---

### Related Information

For information on related concepts:

- [Authentication](#)

For information on related tasks:

- [Authentication Configuration Guide](#)

# Configuring a Windows Server 2000 or 2003 for RADIUS Authentication

---

This Help topic provides instructions for users who wish to configure a Windows 2000 Advanced Server or Windows Server 2003 to provide RADIUS authentication. It includes steps for configuring the Internet Authentication Service (IAS), and for creating users in Active Directory. Policy Manager has been designed to work with a RADIUS server for authentication. The IAS implements the RADIUS protocol, and provides authentication of users connecting to the network via LAN, virtual private network (VPN), and dial-up technology.

It is recommended that you begin by reading the Policy Manager [Authentication Configuration Guide](#) for general authentication instructions prior to following the steps here. Windows 2000 Advanced Server and Windows Server 2003 users should follow the steps in this topic, instead of the Installing and Configuring the RADIUS Server section in the Authentication Configuration Guide.

The recommended sequence for performing the configuration is listed below. When you have completed these instructions, refer back to the sections [Configuring RADIUS in Policy Manager](#) and [Testing Authentication](#) in the Authentication Configuration Guide for instructions on how to use Policy Manager to configure authentication parameters on your devices, and verify that the users created in Active Directory can authenticate to the network.

---

**NOTE:** The following instructions assume that you already have IAS installed on your computer.

---

Instructions on:

1. [Configuring Internet Authentication Service \(IAS\)](#)
  - a. [Specifying RADIUS Port Numbers](#)
  - b. [Adding RADIUS Client Devices](#)
  - c. [Adding a New Remote Access Policy](#)
  - d. [Registering IAS](#)
  - e. [Stopping and Restarting IAS](#)

2. [Creating Users in Active Directory](#)
  - a. [Creating a User](#)
  - b. [Specifying User Permissions](#)
3. [Configuring Devices and Testing Authentication](#)

---

## Configuring Internet Authentication Service (IAS)

---

**NOTE:** Install the latest service pack, which is available at the Microsoft website, before configuring authentication for Windows 2000 Advanced Server or Windows Server 2003. The following instructions assume that you already have IAS installed on your computer.

---

### *Specifying RADIUS Port Numbers*

Use the following steps to specify the RADIUS authentication and accounting port numbers.

1. Select **Start > Programs > Administrative Tools > Internet Authentication Service**. The Internet Authentication Service window opens.
2. Right click on "Internet Authentication Service (Local)" and select Properties.
3. In the RADIUS Tab (for Windows 2000 Advanced Server) or the Ports Tab (for Windows Server 2003), enter **1645** in the Authentication field and **1646** in the Accounting field.
4. Click **OK**.

### *Adding RADIUS Client Devices*

Follow these steps to add RADIUS clients (Policy Manager devices, not end users) to the server.

1. In the Internet Authentication Service window (Start > Programs > Administrative Tools > Internet Authentication Service), right click on the Clients folder (for Windows 2000 Advanced Server) or the RADIUS Clients folder (for Windows Server 2003), and select New > Client.
2. Enter a Friendly Name and Protocol and then click **Next**.
3. Enter the IP address of the RADIUS client and select a Client Vendor (e.g. RADIUS Standard).

4. Enter a shared secret. A shared secret is a string of characters that will be used to encrypt and decrypt communications between the RADIUS server and the device (RADIUS client). Without the shared secret, the server and client will be unable to communicate, and authentication attempts will fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not. Be sure to write the shared secret down, as you will be adding it to the RADIUS client devices later.
5. Click **Finish**.
6. Repeat until all of your Policy Manager devices have been added.

### *Adding a New Remote Access Policy*

Follow these steps to add a new Remote Access Policy. A Remote Access Policy is a set of actions which is applied to a group of users that meet a specified set of conditions.

---

**NOTE:** For information on configuring end user VLAN ID attributes (in compliance with RFC 3580) to be used in conjunction with [VLAN to Role Mapping](#), refer to your device firmware and RADIUS server documentation.

---

1. In the Internet Authentication Service window (Start > Programs > Administrative Tools > Internet Authentication Service), right click on the Remote Access Policies folder and select New > Remote Access Policy.
2. **Windows 2000 Advanced Server:** Enter a Policy friendly name and then click **Next**.  
**Windows Server 2003:** Enter a Policy friendly name, select the "Set up a Custom Policy" radio button (as opposed to selecting the Wizard), and then click **Next**.
3. Follow these steps to add a condition. For example, to add a Windows Group condition:
  - a. Click the **Add** button to open the Select Attribute window.
  - b. Select "Windows Groups" and click **Add**.
  - c. Click **Add** in the Groups window.
  - d. Select a domain group (i.e. Domain Users) and click **Add**. Click **OK**.
  - e. Add more groups if needed in the Groups window. Otherwise, click **OK**.
  - f. Click **Next**.

4. In the Permissions window, select "Grant remote access permission" and click **Next**.
5. Add a User Profile for users who match the conditions you have specified:
  - a. Click the **Edit Profile** button to open the Edit Dial-in Profile window.
  - b. In the Authentication tab, select the appropriate authentication methods.
  - c. In the Advanced tab, remove all parameters, such as "Server-Type" and "Framed-Protocol" and click **Add** to add a Filter-Id attribute.
  - d. In the Add Attributes window, select "Filter-Id" and then click **Add**.
  - e. In the Multivalued Attribute Information window, click **Add**.
  - f. In the Attribute Information window, enter the attribute value:  
**Enterasys:version=1:mgmt=su:policy=[role]**  
where [role] is the role name to be applied to this user.

---

**CAUTION:** Include `:mgmt=su` in the string only for users who should have administrative privileges and the ability to telnet to devices and/or use local management on devices when authentication is enabled. For other users, leave it out.

---

6. Click **OK** to proceed through the windows and **Finish**.

### *Registering the IAS*

Follow these steps to register the Internet Authentication Service in the Active Directory, which enables IAS to authenticate users in the Active Directory.

1. In the Internet Authentication Service window (Start > Programs > Administrative Tools > Internet Authentication Service), right click on the "Internet Authentication Service (Local)" and select Register Service in Active Directory.
2. Click **OK**.

### *Stopping and Restarting the IAS*

After completing the above steps to configure the Internet Authentication Service, you must stop and restart the Service.

1. In the Internet Authentication Service window (Start > Programs > Administrative Tools > Internet Authentication Service), right click on the

"Internet Authentication Service (Local)" and select "Stop Service".

2. Right click on the "Internet Authentication Service (Local)" and select "Start Service".

## Creating Users in Active Directory

Use these steps to create users and specify user permissions.

### *Creating a User*

Create a new object for each user who will be authenticating.

1. Select **Start > Programs > Administrative Tools > Active Directory Users and Computers**. The Active Directory Users and Computers window opens.
2. Right click on the left-panel Users folder and select **New > User**.
3. Proceed through the windows, entering the user name, password and other relevant information. Click **Finish**.

### *Specifying User Permissions*

The steps for specifying user permissions are different depending on whether you are using Windows 2000 Advanced Server or Windows Server 2003.

#### **Windows 2000 Advanced Server**

The steps to specify user permissions depends on your domain operation mode. There are two domain operation modes in Active Directory: Mixed Mode and Native Mode. In Mixed Mode, user permission is specified in the User Properties window. In Native Mode, user permission is specified in the [Remote Access Policy](#) that is configured in the Internet Authentication Service. To change the domain operation mode, consult the Microsoft Windows 2000 Advanced Server documentation for guidance.

- **Mixed Mode:**

1. Right click on a user and select Properties. The User Properties window opens.
2. In the Dial-In tab, select either the "Allow access" or the "Deny Access" radio button in the Remote Access Permission (Dial-in or VPN) section.
3. Click **OK**.



- **Native Mode:**

1. Right click on a user and select Properties. The User Properties window opens.
2. In the Dial-In tab, select the "Control access through Remote Access Policy" radio button in the Remote Access Permission (Dial-in or VPN) section.
3. Go to the appropriate policy configured in the Internet Authentication Service and check either the "Grant remote access permission" or "Deny remote access permission" radio button in the policy's Properties window.
4. Click **OK**.

### Windows Server 2003

For Windows Server 2003, user permission is specified in the [Remote Access Policy](#) that is configured in the Internet Authentication Service.

1. Right click on a user and select Properties. The User Properties window opens.
2. In the Dial-In tab, select the "Control access through Remote Access Policy" radio button in the Remote Access Permission (Dial-in or VPN) section.
3. Go to the appropriate policy configured in the Internet Authentication Service and check either the "Grant remote access permission" or "Deny remote access permission" radio button in the policy's Properties window.
4. Click **OK**.

## Configuring Devices and Testing Authentication

When you have completed the above instructions, refer to the sections [Configuring RADIUS in Policy Manager](#) and [Testing Authentication](#) in the Authentication Configuration Guide for instructions on how to use Policy Manager to configure authentication parameters on your devices, and verify that the users created in Active Directory can authenticate to the network.

---

### Related Information

For information on related concepts:

- [Authentication](#)

For information on related tasks:

- [Authentication Configuration Guide](#)

# Policy Manager Concepts

---

This topic explains some of the concepts you'll need to understand in order to make the most effective use of Policy Manager.

Information on:

- [Policy](#)
- [Role](#)
  - [What is a Role](#)
  - [Default Role](#)
- [Policy Domains](#)
- [Service](#)
- [Rule](#)
  - [What is a Rule](#)
  - [Disabling Rules](#)
  - [Conflict Checking](#)
- [Authentication](#)
  - [Authentication Types](#)
  - [RADIUS Authentication](#)
  - [How Authentication Works](#)
  - [Port Authentication States](#)
  - [Port Mode](#)
  - [Configuring Authentication in Policy Manager](#)
- [Packet Tagging](#)
- [VLAN to Role Mapping](#)
- [Dynamic Egress](#)
  - [Setting Domain GVRP Status](#)
- [Policy VLAN Islands](#)
- [MAC Locking](#)
- [Traffic Mirroring](#)
- [Device Groups](#)

- [Port Groups](#)
- [Network Resource Groups](#)
  - [Network Resource Topologies](#)
- [Verifying](#)
- [Enforcing](#)
- [Controlling Client Interactions with Locks](#)

## Policy

In Policy Manager, network access policies are called Roles. See [Role](#), below, for a description.

## Role

### What is a Role

A role is a set of network access services that can be applied at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates. Roles are usually named for a type of user such as Student or Engineering. Often, role names will match the naming conventions that already exist in the organization. A role can contain any number of [services](#) in Policy Manager.

A role may also contain default access control (VLAN) and/or class of service (priority) characteristics that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any access control or class of service defaults, determine how all network traffic will be handled at any network access point configured to use that role.

### Default Role

Once you have created a role, you can assign it as the default role for a port (see [Assigning Default Roles to Ports](#)). The default role becomes the current role for the user on a port if:

1. unauthenticated behavior is set to "Default Role," *and*
2. either of these cases is true:
  - authentication behavior is set to "inactive," *or*
  - authentication behavior is set to "active" but the user fails to authenticate.

If authentication is disabled on a port, the default role is the only way policy can be assigned to an end user. You can view the ports for which the role is the default role on the role [Ports tab](#), and use the **View/Edit Ports** button to make default role changes.

## Policy Domains

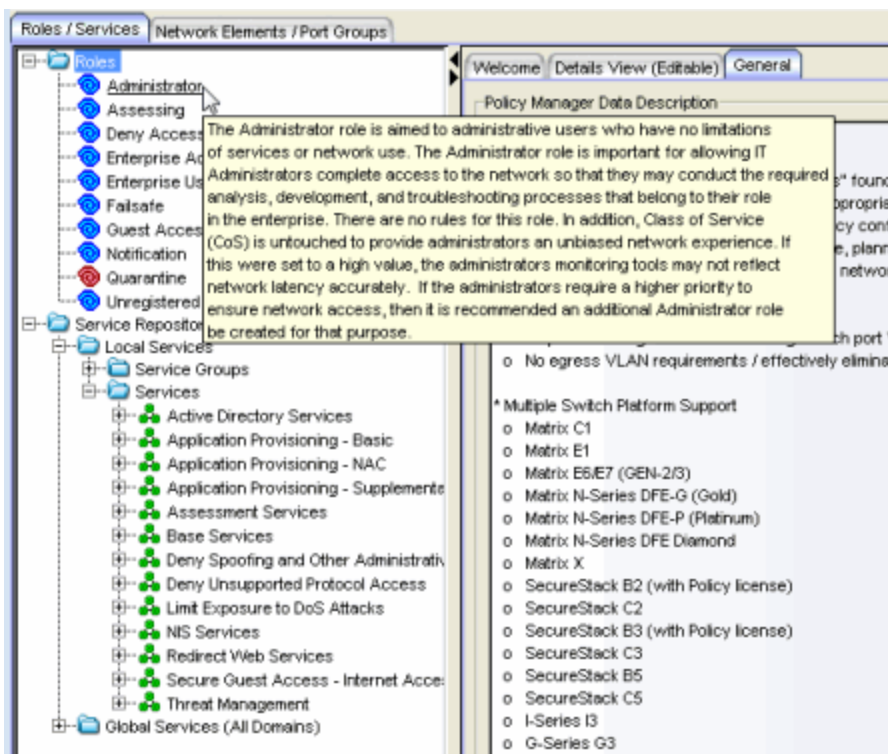
Policy Manager provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between Policy Manager clients.

In Policy Manager, you work in one current domain at a time. Each domain is identified by a unique name. The Domain menu lets you easily switch from one domain to another. There is no limit to the number of domains you can create, however, a device can exist in only one Policy Domain.

The first time you launch Policy Manager, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. By default, the Default Policy Domain is pre-loaded with a Policy Manager Database file called Demo.pmd. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and will often need customization to fully leverage the power of a policy-enabled network.

Policy Manager ships with a set of Policy Manager Database files (.pmd files) that provide ready-made workflows for common policy scenarios. Each .pmd file contains all the elements (roles, services, rules, VLAN membership, class of service) that define how network traffic is handled for each scenario. Policy Manager automatically creates domains for each of these .pmd files, and you can see these domains listed on the Domain menu.

As you look at a domain, use the extensive tool tips to view specific information about the different roles and services (a role tooltip is shown below).



You can import data elements from one domain into another domain. You can also import data from a Policy Manager Database file (.pmd file) into a domain, and you can export data to a .pmd file, (one file per domain) for backup and troubleshooting purposes. Verify and Enforce operations are performed only on the current domain.

In order for your network devices to be displayed in the Policy Manager Network Elements tree, they must be assigned to a Policy Domain. Initially, you must use Console to add your devices to the Extreme Management Center database. Once devices have been added to the Management Center database, you can assign the devices to a Policy Domain using Policy Manager. As soon as a device is assigned to a domain, it is automatically displayed in the Policy Manager Network Elements tree. Only devices that support policy are displayed in the Policy Manager tree.

Policy Manager automatically locks the current Policy Domain when you begin to edit the domain configuration. Other Policy Manager clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released. For more information, see [Controlling Client Interactions with Locks](#). After a Policy Domain has been changed, you must save



the domain to notify all clients that are viewing that domain of the change and automatically update their view with the new configuration.

## Service

Policy Manager services are sets of [rules](#) that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. Policy Manager allows you to create Local Services (services that are unique to the current domain) and Global Services (services that are common to all domains). Global Services let you easily create and manage services that are shared between all your domains. A service can be included in any number of [roles](#) in Policy Manager.

As an example, you might create a service called "High Priority Internet Web Access" that contains priority classification rules for traffic directed toward each of your organization's Internet proxy servers. This service would likely contain one traffic classification rule for each of your Internet proxy servers.

Services can be one of two types: Manual Service or Automated Service.

- **Manual Service**  - This service consists of one or more [traffic classification rules](#) that you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- **Automated Service**  - This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group. You create a network resource group using a list of IP addresses or an IP subnet, and then associate the group with the Automated service (see [How to Create a Network Resource Group](#) for more information). Automated rule types include Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

Policy Manager services provide a common language that network engineers, information technology administrators, and business managers understand. See [How to Create a Service](#) for more information.

## Rule

### What is a Rule

In Policy Manager, a rule defines one element of how traffic for a particular network service or application will be handled by a network access device. For example, you might create a rule that assigns a certain priority to all email traffic, by adding an 802.1p, ToS, or DiffServ value to all SMTP traffic. In Policy Manager, a rule can be included in any number of [services](#), and you can select the types of devices to which the rule applies.

See [Traffic Classification Rules](#) for a detailed explanation of rules.

### Disabling Rules

In Policy Manager, you can elect to disable a rule during or after its creation. If you disable a rule, it is temporarily unavailable for use by the current service, but it can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is a way to temporarily remove a rule from your service without having to delete and recreate it.

### Conflict Checking

As you create your Policy Manager services and rules, there is a possibility that you will define conflicting rules. A conflict exists when two rules in the same service or role define different actions for the same traffic description. For example, two rules might have the same traffic description, but forward traffic to different VLANs, or have different priorities. Policy Manager ensures that conflicting rules do not coexist in the same role or service by checking rule traffic descriptions and action values, providing a message if conflicts are found, and writing the conflict information to the Event Log. If a rule is [disabled](#), conflicts between that rule and others are ignored.

The one exception to this conflict checking behavior, is when the conflicting rules coexist in the same role, but one rule exists in a Local service and the other exists in a Global service. In this case, the rule defined in the Local service takes precedence over the rule defined in the Global service because the Local service is specific to the current domain. Consider the following example:



In the North Campus domain you have a Local service "A" that assigns an Ethertype IP rule to the Red VLAN. The "A" service is assigned to the Student Role. In addition, a Global service "B" exists that assigns Ethertype IP rules to the Blue VLAN. The "B" service is also assigned to the Student Role. In this case, the Local service takes precedence over the Global service in the North Campus domain. Note that the precedence pertains to the rule's actions: class of service (priority) and access control (VLAN). For example, if a rule in a Local service and a rule in a Global service both have the same traffic description, and the Local rule's actions apply CoS Priority 1 and no access control (no VLAN), while the Global rule's actions apply CoS Priority 2 and VLAN Blue(2), then the rule will be enforced using CoS Priority 1 and VLAN Blue(2). In addition, if *either* the Local or Global service has the Accounting or Security actions enabled, then they will be enforced to the devices.

## Authentication

Authentication is the process by which end users identify themselves to the network and are given customized access capabilities based on the role they serve in the organization.

In the past, the IP address has been a means of identifying users on a network. But the mobility of today's workforce and the dynamic nature of IP address assignment has rendered the IP address ineffective as an indicator of the user's identity. Authentication via the user's login has become the most viable option for discovering a user's identity, and provides a mechanism by which policy may be enforced, as well.

## Authentication Types

Policy Manager offers the following types of authentication. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User Authentication). Refer to the Firmware Support tables for information on the authentication types supported by each device type.

### *Web-based Authentication (PWA or Port Web Authentication)*

With Web-based Authentication, users wishing to receive network services access a secure web page from a browser, and supply a user name and

password that is sent to the authentication server. In return, the authentication server supplies a predetermined role for that user based on the user name.

The process is as follows: The user authenticates by typing the Web Authentication URL or IP address into a browser, which then downloads a web page from the switch. A user name and password is entered into the page and sent to the switch, which forwards the request to a RADIUS server. The RADIUS server responds with a filter ID which corresponds to a role. The switch then applies the role to the port, which allows the user to access the DHCP server for a more permanent IP address, and receive the services required.

---

**NOTE:** End users who use DHCP will get a temporary IP address from the switch in the form `192.168.1.Port_Number`. This IP address provides access to the authentication login web page. If authentication is successful, the end user can obtain a permanent IP address from the DHCP server. End users who use static IP addresses must be on the 192.168.0.0 network (with a mask of 255.255.0.0) or have a route to it. Otherwise, they will not be able to access the authentication login web page for authentication.

---

For information on configuring the components required for web-based authentication using Policy Manager, see the [Authentication Configuration Guide](#).

### *802.1X Authentication*

With 802.1X authentication, no Web Authentication URL is used; rather, the login process is combined with the operating system's login process. The credentials supplied by the user during the operating system login are used to do the authentication.

The process is as follows: The end station running 802.1X connects to the switch, and the switch sends out an EAP (Extensible Authentication Protocol) challenge. The end station responds with an EAP response containing the user credentials, which the switch forwards to a RADIUS server. The RADIUS server passes the request to an authentication server, and the authentication server relays the results back to the RADIUS server. Upon successful authentication, the RADIUS server sends an EAP response with a filter ID which corresponds to a role, back to the switch. The switch then applies the role to the port, which allows the user to receive the appropriate services. With 802.1X authentication, you can set up periodic automatic re-authentication of logged-in users without disrupting their sessions.

For information on configuring the components required for 802.1X authentication using Policy Manager, see the [Authentication Configuration Guide](#) and the [802.1X Authentication Configuration Supplement](#).

### *MAC Authentication*

For devices that support this feature, MAC authentication provides a means of authenticating without the user login required by the web-based and 802.1X methods. On the device, you specify a MAC password which will be used for all MAC addresses connected to that device. On the RADIUS server, instead of entering user names, you enter the MAC addresses which are allowed to authenticate, and enter the appropriate MAC password for every MAC address. Then, when a MAC address attempts to access a port, the device sends the MAC address and the MAC authentication password to the RADIUS server for authentication. Automatic re-authentication is available with MAC authentication.

For information on configuring the components required for MAC authentication using Policy Manager, see the [Authentication Configuration Guide](#).

---

**NOTE: Single User 802.1X+MAC Authentication.** On Matrix E1 and Matrix E6/E7 devices, if both 802.1X and MAC authentication are enabled on a device, it is possible for the device to receive a start or response 802.1X packet while a MAC authentication is in progress. If this happens, the device immediately terminates the MAC authentication, and the 802.1X authentication proceeds to completion. Regardless of the success of the 802.1X login attempt, no new MAC authentication logins may occur on the port until 1) the link is toggled; 2) the user executes an 802.1X logout; or 3) the 802.1X session is terminated administratively.

---

### *CEP Authentication*

For devices that support this feature, CEP (Convergence End Point) authentication provides support for CEP products such as IP phones. To configure CEP authentication, you select the CEP product types supported on a device, and map a role for each type. Then, when a convergence endpoint (such as an IP phone) connects to the network, the device identifies the type of endpoint and applies the assigned role. In addition to configuring CEP on a device, you must also enable CEP protocols on each port. Once you have configured CEP on the device and each port, you can monitor CEP product activity using Policy Manager's Port Usage tabs.

For information on configuring the components required for CEP authentication, see the [Authentication Configuration Guide](#).

### *Quarantine Authentication*

Quarantine authentication allows you to assign a Quarantine role to an authenticated end user, thereby limiting or denying their ability to access the network. If an end user's traffic appears to be malicious, this enables you to quarantine the end user until further action can be taken.

Quarantine authentication works in conjunction with quarantine policy rules that assign a Quarantine role to the end user as part of their rule actions. When an end user authenticates to the network and is assigned a role, if their traffic matches a quarantine rule, they will be assigned a Quarantine role. The Quarantine role then restricts or prevents additional traffic from that user from entering the network, according to how the role is configured.

For example, let's say an authenticated end user is acting as a rogue DNS server on the network. Since a DNS server maps hostnames to IP addresses, this would allow them to direct traffic somewhere other than the legitimate destination. If the role assigned to the end user includes a quarantine rule that denies DNS traffic, the end user's traffic would be dropped and they would be assigned a Quarantine role to restrict or stop their access to the network. The end user will have to contact the administrator to regain access to the network.

For information on configuring the components required for Quarantine authentication, see the [Authentication Configuration Guide](#) and [How to Configure Quarantine Authentication](#).

### *Auto Tracking*

Auto tracking is a form of authentication that is used to track session information for traffic that is not authenticated by the other supported authentication types (802.1x, PWA, MAC, CEP, and Quarantine). With auto tracking enabled, these sessions are entered into the session table, allowing network administrators to determine which end-systems on which ports are not being authenticated through traditional authentication methods.

When an end-system connects and does not authenticate using any of the other authentication methods, an auto tracking session is created. The end-system is assigned the appropriate policy as configured in Policy Manager, such as the port's default role.

Auto tracking provides the administrator with increased visibility into who is on the network and where. Because these sessions are tracked, an administrator can determine whether and how to provision them in the future, allowing for increased security and control.

For information on configuring the components required for Auto Tracking authentication, see the [Authentication Configuration Guide](#) and [How to Configure Quarantine Authentication](#).

---

**CAUTION:** Auto tracking authentication should not be used in domains that use MAC to role mappings or IP to role mappings that are based on destination MAC or IP addresses. For more information, see [Auto Tracking and Destination Role Mappings Compatibility](#).

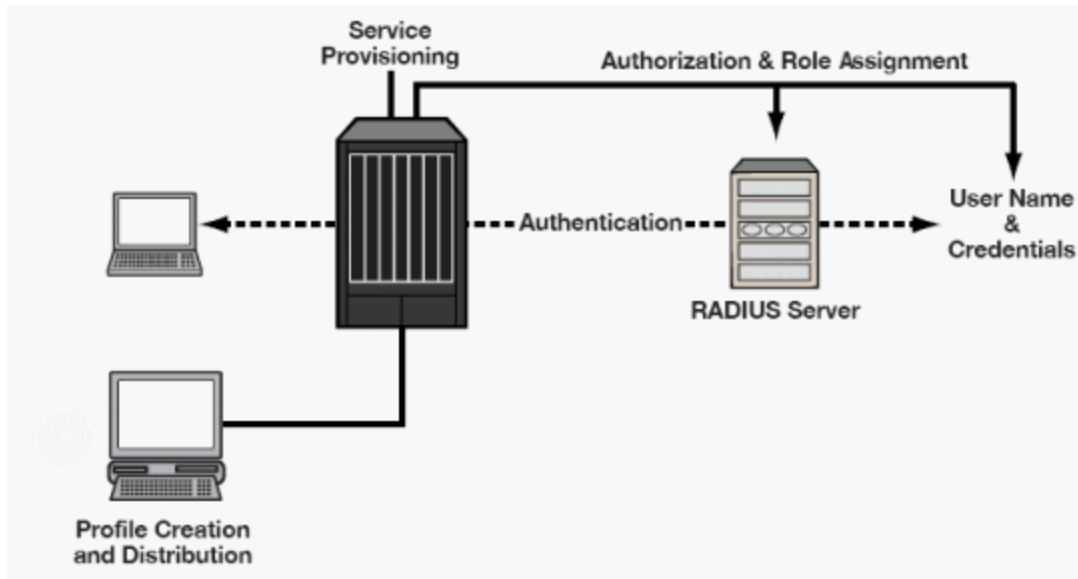
---

## RADIUS Authentication

Policy Manager uses a RADIUS server and an authentication-enabled switch to allow the active policy (or role) on a port to be dynamically assigned, based on the user's login. It exchanges information between a RADIUS client (a device that provides network access to users) and a RADIUS server (a device that contains authentication information for these users).

## How Authentication Works

If authentication is enabled on a network port, a user connected through that port may not be allowed to access network resources unless the user's user name and password are authenticated by the RADIUS authentication server. The unauthenticated port may be configured with some default access permissions, through the use of a default role, or the port may be configured to deny all network access until a user authenticates.



When a user logs in, the RADIUS server is contacted to determine whether or not a policy profile (role) exists for the user in its database. If a role exists, the user is allowed to access the network, and that user's role becomes the current role for the port. If authorization fails, the user is not allowed on the network, and the port assumes the default role for the port. (Only one default role is allowed per port.) Once a role is assigned to a port, the port's current role takes precedence over its default role, and the only way it can be replaced with another role is via authentication, or if the user logs out.

There are some devices within an IT system that may not be configured for authentication. These include printers, FAX machines, and legacy devices such as software-based routers and shared hubs. You can configure default network behavior for these devices in Policy Manager by assigning default roles to the desired network ports or port groups. (See [Assigning Default Roles to Ports](#) for more information.)

## Port Authentication States

When deploying an authentication-enabled network, there are three primary port authentication states that can exist:

- **Authentication off/Port on** - This is simply the network behaving the way it would without authentication. Authentication is not required, and there may or may not be static policy rules applied.
- **Authentication on/Port off** - This occurs when users must authenticate to the interface prior to getting any kind of connectivity. It is the strictest of

the port states, as the user can neither send nor receive any network traffic, except for authentication traffic, until he or she has successfully authenticated to the system

- **Authentication on/Port on with default policy** - This involves the enabling of authentication on the interface, but allowing certain traffic to traverse that interface, either prior to authentication, or after a failed attempt to authenticate. In this scenario, it is likely that users would be allowed to use basic network services, such as Internet, or NOS login, but not access other areas of the network, or consume large amounts of network bandwidth. Alternately, all of the ports that don't have authenticated users might restrict all of their traffic to a lower priority until they authenticate. This allows the network administrator to allow basic network connectivity to users that need it, such as consultants, or temporary employees but to not expose them to all of the organization's resources and available services.

You can control the state of a port with regard to authentication by defining its port mode in Policy Manager.

## Port Mode

Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned the port's [default role](#) or discarded).

- **Authentication Behavior** -- Defines whether or not end users are required to authenticate on the port (device).
  - **Active** -- Normal authentication procedures are implemented. End users are required to authenticate.
  - **Inactive** -- Authentication of end users is not required.
- **Unauthenticated Behavior** -- Defines how the traffic of unauthenticated end users will be handled on the port.
  - **Default Role** -- If the end user is unauthenticated, the port will implement its default role. If there is no default role, there will be no role on the port.
  - **Discard** -- If the end user is unauthenticated, no traffic is allowed on the port.

These two settings can be combined to create four possible port modes.

- **Inactive/Discard Mode:** In this mode, authentication is inactive for the port. All traffic from users connected to the port is discarded. This effectively turns the port off. This port mode is not available for Single User MAC Authentication.
- **Inactive/Default Role Mode:** In this mode, authentication is inactive for the port. All users connecting to this port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. This is the default port mode for ports.
- **Active/Discard Mode:** In this mode, authentication is active for the port and end users are required to authenticate. All traffic from unauthenticated users connected to the port is discarded. The Unauthenticated Behavior varies depending on the type of authentication configured on the device.

*Single User Web-based Authentication:* If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

*Single User 802.1X and 802.1X+MAC Authentication:* If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. This mode requires that there be **no** default role assigned to the port.

*Single User MAC Authentication:* This port mode is not available for Single User MAC Authentication.

*Multi-User 802.1X and MAC Authentication:* If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

*Multi-User Web-based Authentication:* This port mode is not available for Multi-User Web-based Authentication.

**Advantages of Active/Discard mode:** This mode is highly secure, since the



end user receives no network services at all until authentication is successful.

**Disadvantages of Active/Discard mode:** The unauthenticated end user is unable to connect to any network services, such as the Domain Controller (if using a Microsoft operating system), DHCP services, DNS services, or the Web proxy. In single user web-based authentication, the device spoofs WINS/DNS services (if the functionality is enabled) in order to allow the user to communicate with it for authentication.

- **Active/Default Role Mode** - In this mode, authentication is active for the port and end users are required to authenticate. If authentication is successful, the port is assigned the end user's role as its current role. All unauthenticated users connected to the port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. For Single User 802.1X and 802.1X+MAC Authentication, this mode **requires** that a default role be assigned to the port.

**Advantages of Active/Default Role mode:** In this mode, a default role is applied to the port to allow unauthenticated end users access to basic services such as the DHCP Server, Domain Services, WINS, and the Web proxy. When the end user is authenticated, that user's role is applied to the port, providing a customized set of services allowed by his or her role. Active/Default Role mode is an alternative to Active/Discard mode, which is limiting in that there are no network services available at all until the end user is authenticated.

**Disadvantages of Active/Default Role mode:** This mode is less secure than Active/Discard, in that the user receives some network access prior to authentication.

It is important to plan in advance the port mode for the ports in your network before implementing authentication in your policy-enabled network. You can configure port mode in the Port Mode window in the [Port Configuration Wizard](#), or in the [Port Properties Authentication Configuration tab](#) for the port. In order for the port mode settings to take effect, authentication must be configured and enabled on the device.

## Configuring Authentication in Policy Manager

In Policy Manager you can configure and enable authentication on your devices using the [Device Configuration Wizard](#), or the [Authentication tab](#) for the device (see [How to Configure Devices](#)). You can configure authentication settings for your ports using the [Port Configuration Wizard](#), or the [Port Properties Authentication Configuration tab](#) for the port (see [How to Configure Ports](#)). Before any authentication settings for ports or port groups will take effect, you need to configure and enable authentication on the devices.

You can view login session information for the ports on a selected device on the device's [Port Usage Tab](#), and for a selected port on the [Port Properties Port Usage Tab](#).

## Packet Tagging

Packet tagging in a Policy Manager environment occurs as follows:

Tagged packets and ingress filtering are processed first. Then, VLAN ID and priority are determined.

- *VLAN ID*: If the packet matches an active VLAN classification rule on the ingress port, the VID (VLAN ID) specified in the matching VLAN classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default VLAN, the default VID from the active role on the ingress port is assigned. If there is no active role and no classification rule matches, the 802.1Q PVID for the ingress port is assigned.
- *Priority*: If the packet matches an active priority classification rule on the ingress port, the priority specified in the matching priority classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default priority, the default priority from the active role on the ingress port is assigned. If there is no active role and no classification rule matches, the 802.1Q\_PPRI for the ingress port is assigned.

The set of classification rules that are active on a port includes statically created rules that specify the ingress port on their port list, as well as any rules established as a result of a role being applied on that port. If the port has no active role and thus no default access control (VLAN) or class of service (priority), untagged packets that do not match any classification rules are assigned a VLAN and priority from the 802.1Q and 802.1p defaults for the ingress port.

For a graphical illustration of the packet tagging process in a Policy Manager scenario, see the [Packet Flow Diagram](#). The packet passes through the decision-making process illustrated in the graphic twice -- once for VLAN tagging and once for priority tagging.

---

**NOTE:** Policy Manager offers a Drop VLAN Tagged Frames feature which, if enabled, drops any VLAN tagged packet arriving at a port. This provides extra security in that it prevents users from, for example, coming in with a card capable of VLAN tagging and attempting to access the network. It is recommended that you enable the Drop VLAN Tagged Frames feature when you set a default role on a port or when you enable authentication on a port, because these things indicate that the port is a user port that should not be transmitting tagged packets. See [Drop VLAN Tagged Frames](#) for more information.

---

## VLAN to Role Mapping

VLAN to Role mapping lets you assign a role to an end user based on a VLAN ID. There are two kinds of VLAN to Role Mapping: Authentication-Based and Tagged Packet.

- **Authentication-Based VLAN to Role Mapping** (RFC 3580) - Provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Authentication-Based VLAN to Role mappings are only configured at the device level (for all devices).

**NOTE:** When configuring Authentication-Based VLAN to role mapping, you must enable RFC3580 VLAN Authorization on the device via the [device Authentication tab](#). In addition, VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the default role (if there is one) or the 802.1Q PVID for the ingress port is assigned. For more information on configuring VLAN ID attributes on the RADIUS server, refer to your device firmware documentation, RFC 3580, and your RADIUS server documentation.

- **Tagged Packet VLAN to Role Mapping** - Provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID.

When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. Tagged Packet VLAN to Role mapping can be configured at the device level (all devices) and at the port level (for an individual port on a device). A VLAN can only be mapped to one role at the device level, but the same VLAN can be mapped to a different role at the port level. A mapping does not have to exist at the device level to be created at the port level, and port-level mappings will override any device-level mappings.

**NOTE: TCI Overwrite Requirement**

- Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a COS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.
- If supported by the device, you can enable TCI Overwrite on a per-port basis in the [Port Properties window General tab](#), or for an individual role in the role's [General tab](#). The stackable devices support rewriting the CoS values but not the VLAN ID.

To configure VLAN to Role Mapping in Policy Manager, use the role's [Mappings tab](#) and/or the VLAN's [General tab](#). Port-level Tagged Packet VLAN to Role mappings are configured via the [Port Properties General tab, Mappings Sub-tab](#). You must have the Port Level Role Mappings feature enabled in Policy Manager for port-level mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, any port-level mappings will be ignored.

## Dynamic Egress

In Policy Manager, you can control whether or not Dynamic Egress is enabled for a VLAN by checking or unchecking the box in the Dynamic Egress area on the [Create VLAN window](#) or on the [General tab](#) for the VLAN. The default setting for Dynamic Egress is enabled.

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. However, GVRP (GARP VLAN Registration Protocol), which automatically adds the interswitch ingress ports to the egress lists of VLANs, can be enabled in Policy Manager. (See [Example 2](#), below.) You can enable GVRP for the domain by selecting the **Edit > GVRP > Enable GVRP** menu option.

**NOTE:** If you do not want GVRP enabled on your network, you can disable it by selecting the **Edit > GVRP > Disable GVRP** menu option. If necessary, you can then manually configure the interswitch ports to do what GVRP does automatically, using local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration. For more information on using GVRP in Policy Manager, see the section on [Setting Domain GVRP Status](#) below.

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

If an endstation is talking to a "silent" endstation which does not send responses, like a printer, you will need to add the silent endstation's ingress port to the VLAN's egress list manually using local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See [Example 4](#), below.)

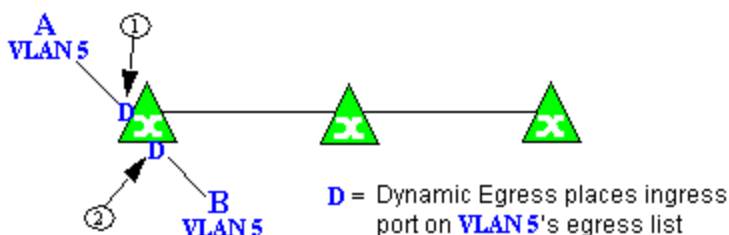
---

**CAUTION:** If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries 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 and B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A 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.

---

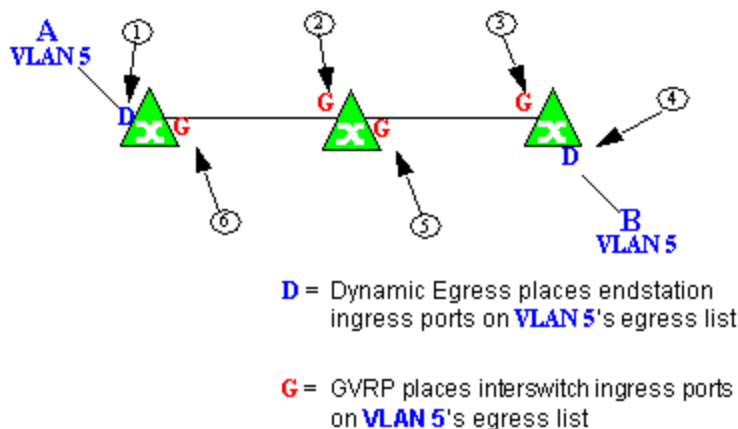
#### *Example 1: Dynamic Egress Enabled*

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.



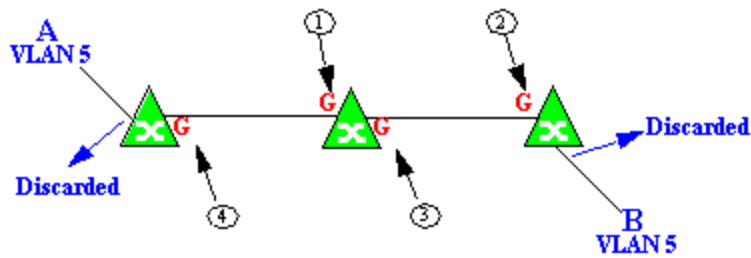
### Example 2: Dynamic Egress + GVRP

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.

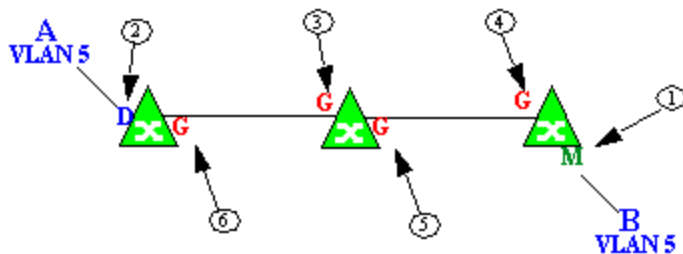


**G** = GVRP places interswitch ingress ports on **VLAN 5**'s egress list

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

#### Example 4: Silent Endstation

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



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

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

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

## Setting Domain GVRP Status

Policy Manager allows you to set the domain GVRP (GARP VLAN Registration Protocol) status via the Edit menu. There are three GVRP status options. To set the GVRP status for all the devices in the current domain, select a status and then enforce.

- **Ignore GVRP** - When this option is selected, Policy Manager will ignore the GVRP configuration on a device during an Enforce operation. This allows you to configure some network switches with GVRP enabled and others with GVRP disabled (using MIB Tools or local management), according to their configuration requirements.
- **Enable GVRP** - When this option is selected, GVRP will be enabled for the devices in the current domain.
- **Disable GVRP** - Select this option if you do not want GVRP enabled on the devices in the current domain. Disabling GVRP may affect connectivity through ports with VLANs that rely on Dynamic Egress. If GVRP is disabled, rules using VLAN containment may not work properly unless the VLANs have been pre-configured on the devices outside of Policy Manager.

The following table shows how domain GVRP status affects device-level and port-level GVRP status when an Enforce operation is performed.

<b>Domain GVRP Status</b>	<b>Device Set on Enforce</b>
Domain GVRP status is set to Ignore.	No GVRP status is written to devices on Enforce.
Domain GVRP status is set to Enable and the device-level GVRP is enabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to Enable and the device-level GVRP is disabled.	Device-level GVRP status and port-level GVRP status is set to enabled on Enforce.
Domain GVRP status is set to Disable and the device-level GVRP is disabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to Disable and the device-level GVRP is enabled.	Device level GVRP status is set to disabled and no change is made to the port-level GVRP status on Enforce.



## Policy VLAN Islands

Policy Manager offers you the ability to set up Policy VLAN Islands which enable you to deploy a policy across your network, while restricting user access to only selected local devices. For example, if you want to have a guest VLAN but you do not want the guests in one facility to be able to communicate with guests in another facility, you can set up a VLAN island containing only selected devices in each facility, with access controlled by island VLANs.

- **Global VLAN** - Global VLANs are written to all selected devices with the same VID. They are referenced in the format <VID[name]>.
- **Island VLAN** - An Island VLAN is a conceptual VLAN and does not have an actual VID. The VID is assigned automatically based on the island it belongs to.

---

**NOTE:** Policy Manager provides management of Global VLAN settings, but does not provide management of Island VLANs beyond setting the appropriate VIDs in the Role defaults and Rule access control actions. Also, you must manage separately other related settings in the qBridgeMib such as name, and dynamic egress values.

---

See [How to Create a Policy VLAN Island](#) for more information.

## MAC Locking

MAC Locking ensures that only specific MAC addresses can access a port, and that traffic from any other MAC addresses will be discarded. You might take advantage of MAC Locking if, for example, you want to prevent more than one user from accessing a port at a given time. There are two kinds of MAC Locking: Dynamic and Static. When you enable Dynamic MAC Locking on a port, the next MAC address that authenticates or accesses the port (up to the maximum number of dynamic locked MAC addresses allowed) will have exclusive access to that port from that time on. Static MAC Locking lets you create a list of locked MAC addresses for a port so that the port only accepts traffic from those MAC addresses. MAC Locking is only available on devices that support it, and is not allowed on backplane and logical ports.

In order for MAC Locking to take effect on a port, it must be enabled at the device level. You can do this using the [Device Configuration wizard](#), or the device [MAC Locking tab](#). You can enable and disable MAC Locking for a

specific port on the [Port Properties MAC Locking tab](#). You can also enable MAC Locking for multiple selected ports in the [Port Configuration wizard](#).

## Traffic Mirroring

Policy Manager provides policy-based traffic mirroring functionality that allows network administrators to monitor traffic received at a particular port on the network, by defining a class of traffic that will be duplicated (mirrored) to another port on that same device where the traffic can then be analyzed. Traffic mirroring can be configured for a rule (based on a traffic classification) or as a role default action. Only incoming traffic can be mirrored using policy-based traffic mirroring, and the traffic mirroring configuration takes precedence over regular port-based mirroring.

Traffic mirroring uses existing Policy Manager port groups (created using the Port Groups tab) to specify the ports where the mirrored traffic will be sent for monitoring and analysis. When an end user connects to the device where the specified ports exist, and is assigned the role that has traffic mirroring configured, then there is a traffic mirror set up for the port the end user connected to. However, if the end user is assigned a role that does not have traffic mirroring configured, or if the end user connects to a device that doesn't have any ports in the specified port groups, then no traffic mirror will exist.

Examples of how traffic mirroring might be used include:

- Mirroring the traffic from suspicious users based on their MAC or IP address.
- Monitoring VoIP calls by IP address or port range.
- Mirroring traffic to optimized IDS systems, for example one system for all HTTP traffic (to look for suspicious websites) or one system for all emails (to look for spam).
- Mirroring traffic to Application Analytics appliances for use in Extreme Management Center application identification reports and analysis.

For information on configuring traffic mirroring, see the [Role General tab](#) and the [Rule General tab](#).

## Device Groups

Policy Manager allows devices to be combined into groups, similar to the way services can be combined into service groups. With device groups, you can perform certain operations on an entire group at once, instead of performing the operation on individual devices. A device can be a member of more than one group.

Policy Manager provides several system-created device groups for your convenience. You can also create your own device groups, called user-defined device groups. Policy Manager system-created device groups are displayed with blue folders. Any group you add will be displayed with a yellow folder. For more information on creating device groups, see [How to Add and Remove Device Groups](#).

### System-Created Device Groups

System-created device groups are located under the My Network folder in the Network Elements tab. When a device is assigned to a domain, it automatically becomes a member of the appropriate group:

- All Devices - contains all the devices that are assigned to the current domain.
- Grouped By - contains five subgroups:
  - Chassis -- contains subgroups for specific chassis in the domain.
  - Contact -- contains subgroups of the devices in a domain based on the system contact.
  - Device Types -- contains subgroups for the specific product families and device types in the domain.
  - IP -- contains subgroups based on the IP subnets in the domain.
  - Location -- contains subgroups of the devices in a domain based on the system location.

### User-Defined Device Groups

You can add your own device groups and subgroups under the My Network folder, however you cannot add groups under the system-created groups. A device group cannot have the same name as another device group at the same

level. You cannot rename or delete a system-created group. A device can be a member of more than one group.

## Port Groups

Policy Manager allows ports to be combined into groups, similar to the way services can be combined into service groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. You can view port groups on the left-panel Port Groups tab.

Policy Manager provides you with several commonly used port groups for your convenience, called [Pre-Defined Port Groups](#). You can also create your own port groups, called [User-Defined Port Groups](#).

## Pre-Defined Port Groups

Policy Manager provides the following commonly used port groups:

- **10/100 Ports** - Ports whose speed is 10/100.
- **All Ports** - All ports on all devices.
- **FTM 1 Backplane Ports** - Ports whose port type is FTM 1 Backplane and CDP FTM 1 Backplane.
- **Frozen Ports** - All ports that have been [frozen](#).
- **Gigabit Ports** - All gigabit ports.
- **Host Data Ports** - The host data ports on devices that allow you to apply policies to these ports.
- **Interswitch Ports** - All ports whose port type is interswitch. In order for a port to be determined to be an interswitch link, at least one supported neighbor discovery protocol needs to be enabled for the switch and port. Supported protocols are CDP (Cabletron Discovery Protocol), LLDP (Link Layer Discovery Protocol), and EDP (Extreme Discovery Protocol).
- **Logical Ports** - All logical ports.
- **Ten Gigabit Ports** - All ten gigabit ports.

Every time one of the Pre-Defined Port Groups is accessed, Policy Manager goes to the devices and retrieves the ports which fit the pre-defined characteristics of the port group. Unlike the port lists for User-Defined Port Groups, Pre-Defined Port Group port lists are not saved in a Policy Manager data (.pmd) file.

## User-Defined Port Groups

Policy Manager also enables you to create your own port groups and select individual ports to add to the group.

## Network Resource Groups

Network Resource Groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. The Policy Manager [Demo.pmd file](#) contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers. Use the Network Resource Configuration window to view and define your network resource groups. See [How to Create a Network Resource](#) for more information.

Once a network resource group has been defined, you can associate it with an [Automated service](#) (see [How to Create a Service](#) for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

## Network Resource Topologies

Network Resource Topologies are used to divide the devices in a domain into groups called islands. Each network resource group specifies a topology and can then define a unique resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate.

For example, you could create a topology called "Campus Printers" that could be used to restrict printer access to only the printers in the building where the end user is physically located. This topology might define islands such as "Library," "Admissions Office," or "Science Building." Each island would include the network devices for that location. Then, in the Network Resource Group that specifies this topology, there would be resource lists that define the printers for each of those islands.

In addition to defining topologies based on physical location (such as geographic region, corporate offices, or campus buildings) a topology could

also be used to define resources based on the departments within a company (such as Sales, IT, or Human Resources).

When you create a topology, it contains a Default Island that includes all the devices in your domain. You can then create additional islands and distribute your devices between the different islands according to your needs. Each device in a domain must belong to one island in each topology. You can set any island as the Default island for new devices that are added to the domain.

## Verifying

The Verify feature lets you verify that the roles in your current domain have been enforced. Verify operations are performed only on the current domain. The Verify operation compares the roles currently in effect ([enforced](#)) on your domain devices with the roles defined in the current Policy Domain.

---

**NOTE:** If you perform a Verify operation following an Import Policy Configuration from Device, the Verify may fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration. Also, when you import device-specific rules, these rules are converted to a Rule Type of "All Devices," and this will cause Verify to fail. If you want the rules to be device-specific, you will have to change their Rule Type via the Rule General tab after the import and prior to Enforce.

---

You can verify using the [Verify \(Global\)](#) button in the toolbar or the [File > Verify Role Set](#) menu option, both of which verify the information on all the devices in the current domain. You can also selectively verify on individual devices or device groups in the domain by right-clicking the device or group in the left panel or in the right-panel Details View tab for the Devices folder or Device Group folder, and choosing **Verify Role Set** from the menu.

After verifying, you see a window that reports any discrepancies. The title bar of the window lets you know if the verify was done on all devices in the domain, or a subset of devices. From this window, you can select **Enforce Preview** to open the [Enforce Preview window](#), where you can view the effects [enforcing](#) the current role set would have, prior to actually enforcing. You can also view the full results of the Verify operation in the event log, which displays any discrepancies and statistics of the operation itself.

---

## Background Verify on Startup

When you launch Policy Manager or open a domain, a background Verify operation is automatically performed on the current Policy Manager domain. Because this operation runs in the background, you still have instant access to Policy Manager and the domain even while the operation is being performed.

When the background Verify operation is complete, a message will appear on the left side of the status bar indicating whether the domain is in sync, whether an enforce is required, or if one or more devices are unreachable and status could not be determined. The full results of the background Verify are also displayed in the event log, similar to a manual verify operation.

If you manually start a Verify operation while the background Verify is running, the Verify operation moves to the foreground and shows a progress bar with the current progress. If a manual enforce is started, the background Verify is canceled, as it is no longer required.

If you do not want Policy Manager to perform background Verify operations, you can deselect the Background Verify on Startup/Domain Open option in the Options [Startup view](#) (Tools > Options).

## Enforcing

In Policy Manager, enforcing means writing role information to a device or devices. Enforce operations are performed only on the current domain. Any time you add, make a change to, or delete a role or any part of it (any of its services and/or rules), the devices in your current domain need to be informed of the change, otherwise the role will not take effect. To determine if the roles currently in effect on your domain devices match the set of roles you have defined in your current Policy Domain configuration, use the [Verify](#) feature.

---


**NOTE: Setting up Profiles and Credentials for Enforce.** All SNMP operations that are performed from the Policy Manager client use the SNMP credentials of the logged-in user. For example, when devices are identified, the credentials associated with the user's group are used to communicate with the devices. However, the Enforce operation occurs on the server and uses the Management Center Administrator profile to communicate with devices. Because of this, the Management Center Administrator profile must have write privileges on the devices that users can enforce.

---

When an Enforce is initiated, the Policy Domain is locked to prevent other clients from enforcing at the same time. Different Policy Domains can be enforced at the same time, but if another user attempts to enforce the same domain at the same time, that user will be notified that the domain is already locked.

To enforce, use the [Enforce \(Global\)](#) button in the toolbar or the [File > Enforce Role Set](#) menu option, both of which write the information to all devices in the current domain. You can also selectively enforce on individual devices or device groups by right-clicking the device or group in the left panel or in the right-panel Details View tab for the All Devices folder or Device Group folder, and choosing **Enforce Role Set** from the menu. Only users that have been assigned the Enforce capability are allowed to perform an Enforce.

Policy Manager's [Enforce Preview window](#) enables you to view the information that will be written to your domain devices, before you actually enforce. This feature is particularly useful if you have devices that only support certain aspects of policy management. The Enforce Preview window appears whenever you initiate an enforce using one of the methods mentioned above, so that you always have a chance to review the effects of enforcing prior to actually performing the enforce. You can control whether or not this view automatically appears with the **Show this view on Enforce** checkbox on the Enforce Preview window, or in Options window [Optional Views](#) (**Tools > Options**). You can also access this window from the **File > Enforce Preview** menu option, and from the **Enforce Preview** button on the confirmation message that appears when a [verify](#) has taken place.

If you've made changes without enforcing and you attempt to close Policy Manager, you'll be asked if you want to enforce before closing. Also, if you have made changes that need to be enforced, the Enforce icon  appears on the status bar at the bottom of the Policy Manager window as a reminder. After enforcing, you see a window that reports any problems.

## Controlling Client Interactions with Locks

Because Policy Manager uses a Client/Server architecture, it is important to maintain a proper sequence of client interactions to ensure a consistent view of Policy Domains among all clients. To do this, Policy Manager uses Server Locks to manage user interactions. When a user begins editing a Policy Domain (for example by assigning devices or adding a role), a lock is acquired for that domain at the server. That lock is not released until the same user saves the domain data. This guarantees a consistent view of that domain for all clients.



Users are given the option of revoking locks held by other users. This protects against the possibility that users may forget they have locked a domain and keep that lock for an extended period of time.

A domain is locked automatically when a user begins to edit the domain data or a user can lock/unlock a domain by clicking the Lock toolbar button. When a domain is locked, the title bar states that the policy data is being edited and specifies the user who has locked the domain. A lock icon also appears in the status bar. Other Policy Manager clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released.

Here are some important things to remember about locks:

- Locks operate on individual Policy Domains. When a user edits a domain, a lock is acquired for that domain and it remains locked until the same user saves the domain data or the lock is revoked by another user. You cannot save a domain that is locked by another user.
- During Enforce, a lock is acquired on the domain which is being enforced. This ensures a consistent view of the domain while it is being used by the server.
- When devices are being assigned to a Policy Domain, multiple domains may be locked concurrently. This will happen if devices from one domain are being reassigned to another domain. In this case, locks for both domains are acquired.
- When a lock is revoked, the last domain save "wins." While consistency is always maintained by the server, the order of domain saves cannot be guaranteed when locks are revoked, and consequently work done by one user may be lost.

You can view server locks for all clients via the Server Information window Locks tab. You can also revoke locks from this panel. For more information, see [Viewing Locks](#).

---

### **Related Information**

For information on related concepts:

- [Traffic Classification Rules](#)

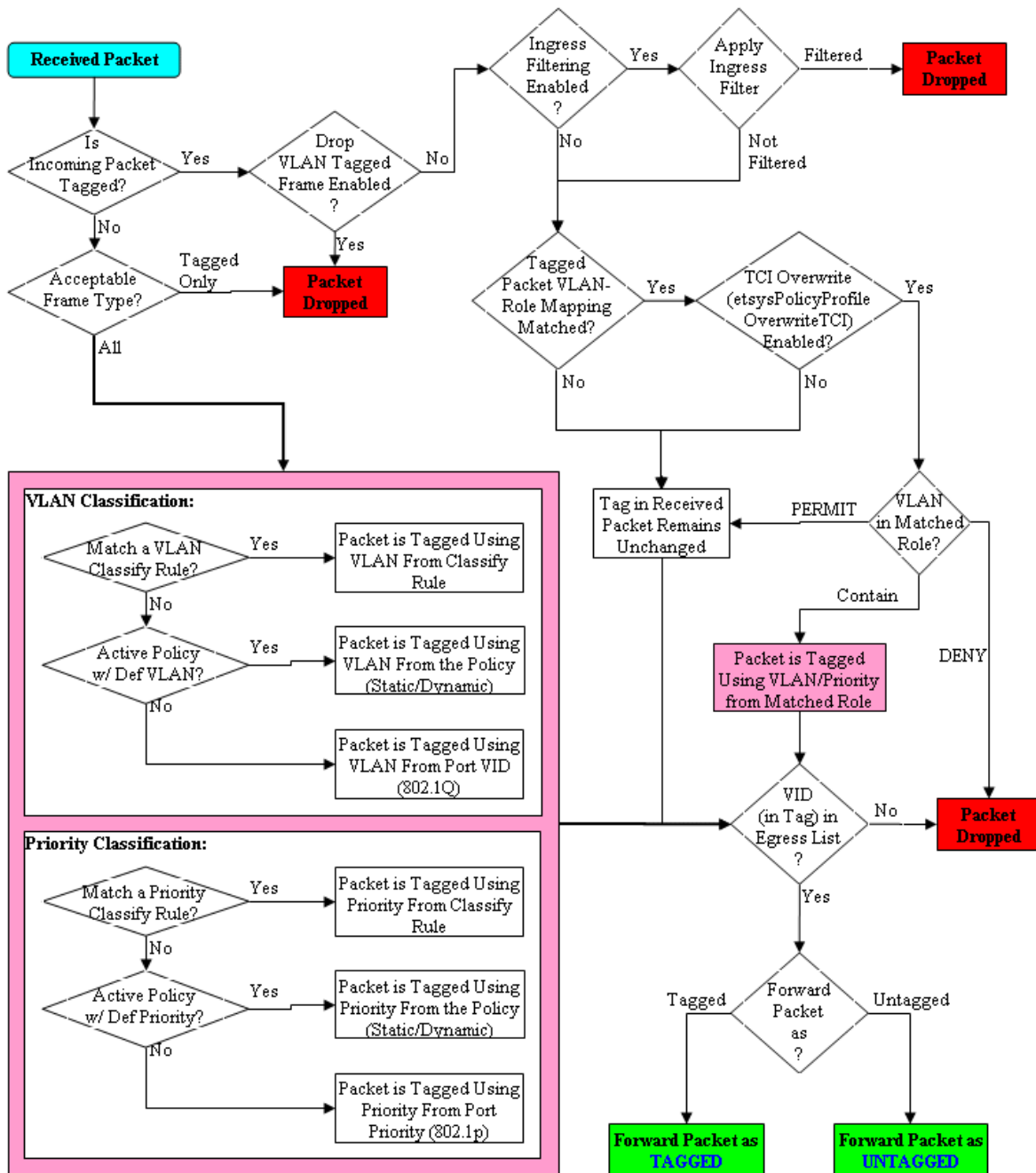
For information on related tasks:

- [Authentication Configuration Guide](#)
- [802.1X Authentication Configuration Supplement](#)
- [Creating a Role Using the Role Wizard](#)
- [How to Configure Devices](#)
- [How to Configure Ports](#)
- [How to Create a VLAN](#)

For information on related windows:

- [Create VLAN Window](#)

# Packet Flow Diagram



## Traffic Classification Rules

---

Traffic Classification rules allow you to assign VLAN membership and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, 4, and 7 of the OSI model, and all network traffic can be classified according to specific layer 2/3/4/7 information contained in each frame. In Policy Manager, rules are used to provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. Examples of how to design rules for each of these features are given below.

A Traffic Classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the traffic classification type for the rule. The Actions specify whether traffic matching that classification type will be assigned VLAN membership, class of service, or both. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame. Use the Policy Manager's [Rule Wizard](#) to quickly and easily create a rule and define its traffic description and actions.

In Policy Manager, rules are created and then grouped together into Services, which are then used to define roles. A role is assigned to each port either through end user authentication or as the port's default role. This means that there can be multiple rules active on a port. When a frame is received on a port, if the frame's classification type matches more than one rule, classification precedence rules are used to determine which rule to use.

The following information is discussed in this file:

- [Traffic Descriptions](#)
- [Actions](#)
  - [VLAN Membership](#)
  - [Priority \(Class of Service\)](#)
- [Classification Types and their Parameters](#)
  - [Layer 2 Data Link Classification Types](#)
  - [Layer 3 Network Classification Types](#)
  - [Layer 4 Application Transport Classification Types](#)
  - [Layer 7 Application Classification Type](#)

- [Examples of How Rules are Used](#)
  - [Traffic Containment](#)
  - [Traffic Filtering](#)
  - [Traffic Security](#)
  - [Traffic Prioritization](#)
- [Classification Rules Precedence](#)
  - [Precedence Scenarios](#)

## Traffic Descriptions

When you create a Traffic Classification rule in Policy Manager, you must define the rule's traffic description. The traffic description identifies the traffic classification type for that rule. You must select a classification type, and then select or enter certain parameters or values for each type.

Classification types are grouped according to Layers 2, 3, 4, and 7 of the OSI model and there are multiple classification types for each layer.

OSI Model
<b>Layer 7 - Application</b>
Layer 6 - Presentation
Layer 5 - Session
<b>Layer 4 - Transport</b>
<b>Layer 3 - Network</b>
<b>Layer 2 - Data Link</b>
Layer 1 - Physical

Specific Layer 2/3/4/7 information contained in each frame is used to identify the frame's classification type. Each layer uses different information to classify frames.

- **Layer 2 Data Link** -- classifies frames based on an exact match of the MAC address or specific protocol type of each frame.
- **Layer 3 Network** -- classifies IP or IPX frames based on specific information contained within the Layer 3 header.
- **Layer 4 Transport** -- classifies IP frames based on specific Layer 4 TCP or UDP port numbers contained in the header.

- **Layer 7 Application** -- classifies frames based on specific Layer 7 application types.

For a complete description of Layer 2, 3, 4, and 7 classifications, refer to [Classification Types and Their Parameters](#).

## Actions

When you create a Traffic Classification rule in Policy Manager, you must define the actions that the rule will perform. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame. Actions specify whether the frame will be assigned VLAN membership (access control) and/or priority (class of service).

### *VLAN Membership (Access Control)*

In your network domains, you can create VLANs (Virtual Local Area Networks) that allow end-systems connected to separate ports to send and receive traffic as though they were all connected to the same network segment. Using traffic classification rules, you can classify a frame based on the frame's classification type to have membership in a specific VLAN, providing important traffic containment, filtering, and security for your network.

For example, a network administrator could use rules to separate end user traffic into VLANs according to protocol, subnet, or application. Rules could also be used to group geographically separate end-systems into job-specific workgroups.

### *Priority (Class of Service)*

Traffic Classification rules allow you to assign a transmission priority to frames received on a port based on the frame's classification type. For example, a network administrator could use rules to assign priority to one network application over another.

Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority. Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

Policy Manager enables you to utilize priority by creating classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default. See [Getting Started with Class of Service](#) for more information.

## Classification Types and their Parameters

When you define a rule's traffic description, you select a classification type, and then select or enter certain parameters or values for each type. Classification types are grouped according to Layers 2, 3, 4, or 7 of the OSI model.

### *Layer 2 -- Data Link Classification Types*

Layer 2 classification types allow you to define classification rules based on an exact match of the MAC address or specific protocol type of each frame.

#### **MAC Address Source, MAC Address Destination, MAC Address Bilateral**

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) MAC address contained in an Ethernet frame. Enter a valid MAC address or click Select to open a window where you can select a MAC address read from your network devices. You can specify a mask, however masking a MAC address is not supported on legacy devices.

#### **Ethertype**

This classification type is based on the specific protocol type of each frame defined in the two-byte Ether type field. Select an Ether type from the list of well-known values, or select **Other** and manually enter a single value in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

<b>Well-known Ethertypes</b>	<b>Values</b>
IP	0x0800
ARP	0x0806
Reverse ARP	0x8035
Novell IPX 1	0x8137
Novell IPX 2	0x8138
Banyan	0x0bad

Well-known Ethertypes	Values
AppleTalk	0x809b
AppleTalk ARP	0x80f3
IPv6	0x86dd
Decnet Phase 4	0x6003

### DSAP/SSAP

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

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

### VLAN ID

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

### Priority

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



## Layer 3 -- Network Classification Types

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

### IP Time to Live (TTL)

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

### IPX Network Source, IPX Network Destination, IPX Network Bilateral

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

### IPX Socket Source, IPX Socket Destination, IPX Socket Bilateral

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

Well-known IPX Socket Types	Values
NCP	1105
SAP	1106
RIP	1107
NetBIOS	1109
Diagnostics	1110
NSLP	36865

Well-known IPX Socket Types	Values
IPX Wan	56868
Other	0-65535

### IPX Class of Service

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. This is a one-byte field used for transmission control (hop count) by IPX routers. Enter a valid IPX Class of Service in decimal form, 0-255. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

### IPX Packet Type

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

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

### IPv6 Address Source, IPv6 Address Destination, IPv6 Address Bilateral

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

### IPv6 Socket Source, IPv6 Socket Destination, IPv6 Socket Bilateral

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

Other, you can enter a range of values.

**TIP:** You can define a new value for a UDP or TCP port number using the [Pre-Defined Well-Known IDs window](#). Once defined, it is available for selection from the list of well-known values when defining the rule's traffic classification type.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514

Well-known UDP/TCP Types	Values
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

### IPv6 Flow Label

These classification types are based on the exact match of the value in the 20-bit Flow Label field in the IPv6 header. This field is used to identify packets belonging to particular traffic flow that needs special traffic handling. Enter a flow label value and sigbits mask.

### IP Address Source, IP Address Destination, IP Address Bilateral

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

### IP Socket Source, IP Socket Destination, IP Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IP address and a UDP/TCP port number (type) contained within the IP header of each frame. Enter an IP address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (UDP/TCP port numbers are defined in RFC 1700.) If you select **Other**, you can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

---

**TIP:** You can define a new value for a UDP or TCP port number using the [Pre-Defined Well-Known IDs window](#). Once defined, it is available for selection from the list of well-known values when defining the rule's traffic classification type.

---

<b>Well-known UDP/TCP Types</b>	<b>Values</b>
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812

Well-known UDP/TCP Types	Values
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

### IP Fragment

This classification type is based on Layer 4 information in fragmented frames. IP supports frame fragmentation, where large frames are divided into smaller fragments and sent wrapped in the original Layer 3 (IP) header. When a frame is fragmented, information that is Layer 4 and above is only present in the first fragment. For example, the first fragment may be classified to Layer 4, while subsequent fragments will be classified only to Layer 3. The product line does not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4 information is not present in these frames. Using the IP Fragment classification rule, any frame which is a fragment of a larger frame, is classified according to the information in the original frame. If the first fragment is classified to Layer 4, subsequent fragments will also be classified to Layer 4.

### ICMP and ICMPv6

These classification types are based on an exact match of the ICMP (Internet Control Message Protocol) message contained in the ICMP tag within a frame. Select an ICMP well-known value type from the list of well-known values (some well-known value types also let you select a code), or select **Other** and manually enter the value in hexadecimal form. The format of the value is 0xXXYY, where "XX" is the ICMP type, and "YY" is the associated code, if applicable. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

### IP Type of Service

This classification type is based on an exact match of the one-byte ToS/DSCP field contained in the IP header of a frame. The ToS (Type of Service) or DSCP (Diffserve Codepoint) value is defined by an 8-bit hexadecimal number between 0 and FF. Enter a value or click Select to open a window where you can generate a hex value. For information on how to generate a ToS or DSCP value, see the [ToS/DSCP Configuration](#) window or the [ToS/DSCP Value Definition Chart](#).

Type of Service can be used by applications to indicate priority and Quality of Service for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service. In many networks, better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases, at most, two of the parameters should be set.

**For a ToS value**, the 8-bit hexadecimal number breaks down as follows:

Bits 0-2: Precedence

Bit 3: 0=Normal Delay, 1=Low Delay

Bit 4: 0=Normal Throughput, 1=High Throughput

Bit 5: 0=Normal Reliability, 1=High Reliability

Bits 6-7: Explicit Congestion Notification

The precedence bits (bits 0-2) break down as follows:

111 - Network Control

110 - Internetwork Control

101 - CRITIC/ECP

100 - Flash Override

011 - Flash

010 - Immediate

001 - Priority

000 - Routine

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway originators only.

**For a DSCP value**, the value represents codepoints for two Differentiated Services (DS) Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

### IP Protocol Type

This classification type is based on the specific protocol type defined in a field contained in the IP header of each frame. Select a protocol from the list of well-known values, or select **Other** and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

**TIP:** You can define a new value for a UDP or TCP port number using the [Pre-Defined Well-Known IDs window](#). Once defined, it is available for selection from the list of well-known values when defining the rule's traffic classification type.

Well-known IP Protocol Types	Values
ICMP	1
IGMP	2
TCP	6
EGP	8
UDP	17
IPv6 (encapsulated in IPv4 packets)	41
RSVP	46
GRE	47
ESP	50
AH	51
ICMPv6	58
EIGRP	88
OSPF	89
PIM	103
VRRP	112
L2TP	115
Other	0-255

### *Layer 4 -- Application Transport Classification Types*

Layer 4 IP classification types allow you to define classification rules based on specific Layer 4 TCP or UDP port numbers contained in the header of an IP frame. You can specify a specific port number or a range of port numbers.

**Note:** Certain devices do not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4 information is not present in these frames. If a device has an FDDI HSIM installed, Layer 4 classification will not be supported for any frames larger than 1500 bytes. Frames larger than 1500 bytes are fragmented internally in the switch. When creating classification rules based on specific Layer 4 information, using the [IP Fragment](#) classification rule will allow fragmented frames to be classified according to the Layer 4 information contained in the original frame.



### IP UDP Port Source, IP UDP Port Destination, IP UDP Port Bilateral

These classification types are based on specific Layer 4 UDP port numbers contained within the header of an IP frame. Select a UDP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (UDP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

**TIP:** You can define a new value for a UDP or TCP port number using the [Pre-Defined Well-Known IDs window](#). Once defined, it is available for selection from the list of well-known values when defining the rule's traffic classification type.

Well-known UDP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143

Well-known UDP Types	Values
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

#### IP TCP Port Source, IP TCP Port Destination, IP TCP Port Bilateral

These classification types are based on specific Layer 4 TCP port numbers contained within the header of an IP frame. Select a TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (TCP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

**TIP:** You can define a new value for a UDP or TCP port number using the [Pre-Defined Well-Known IDs window](#). Once defined, it is available for selection from the list of well-known values when defining the rule's traffic classification type.

Well-known TCP Types	Values
FTP Data	20
FTP	21

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

Well-known TCP Types	Values
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

### IP UDP Port Source Range, IP UDP Port Destination Range, IP UDP Port Bilateral Range

These classification types are based on Layer 4 UDP port numbers contained within the header of an IP frame. When you select this type, you enter a range of UDP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. UDP port numbers are defined in RFC 1700.

### IP TCP Port Source Range, IP TCP Port Destination Range, IP TCP Port Bilateral Range

These classification types are based on Layer 4 TCP port numbers contained within the header of an IP frame. When you select this type, you enter a range of TCP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. TCP port numbers are defined in RFC 1700.

## *Layer 7 -- Application Classification Types*

Layer 7 IP classification types allow you to define classification rules based on specific Layer 7 application types.

### Application

This rule type allows management of traffic for a specific application type, for example Apple traffic (Bonjour) using mDNS-SD. The following application types are supported:

- LLMNR - (Link Local Multicast Name Resolution) Query/Response  
This protocol is based on the Domain Name System (DNS) packet format. It allows hosts to perform name resolution for hosts on the same local link.
- SSDP - (Simple Service Discovery Protocol) Query/Response  
SSDP is a Universal Plug-and-Play (UPnP) based protocol. SSDP uses the NOTIFY and MSEARCH HTTP methods to discover and advertise services on the network.
- mDNS-SD - (Multicast Domain Name System - Service Discovery) Query/Response  
DNS-SD is a service discovery protocol that utilizes the Domain Name

System. Multicast DNS is a protocol that is mostly compatible with normal DNS but uses link local multicast addressing, allowing for zero configuration networking (zeroconf) functionality.

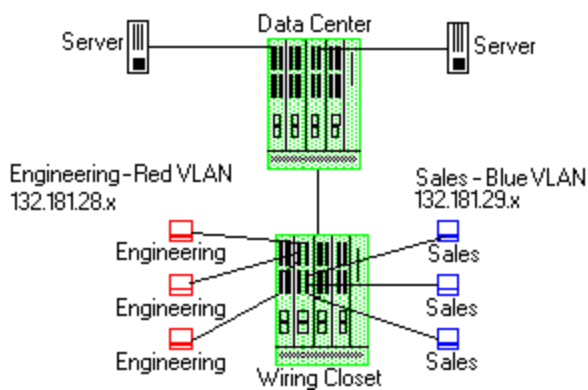
## Examples of How Rules are Used

Traffic Classification rules are used to provide four key policy features: Traffic Containment, Traffic Filtering, Traffic Security, and Traffic Priority.

### *Traffic Containment*

Using classification rules, network administrators can group together users of a given protocol, subnet, or application, and control where their traffic can logically go on the network.

#### IP Traffic Containment



The figure above shows a configuration where the network administrator wants to separate end-user traffic into VLANs based on the assigned IP subnet of each department. This can easily be accomplished by creating two Layer 3 classification rules based on the IP subnet range of the respective departments.

Rule 1 - Engineering, which uses the 132.181.28.x subnet, will be assigned to the Red VLAN.

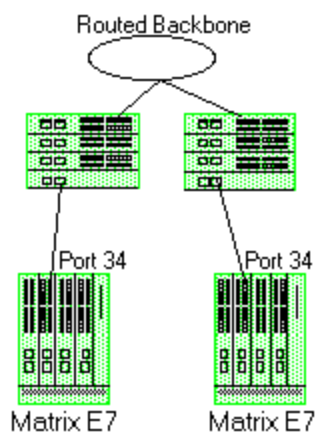
Rule 2 - Sales, which uses the 132.181.29.x subnet, will be assigned to the Blue VLAN.

Based on these two Layer 3 classification rules, the traffic from the Engineering VLAN will be isolated from the Sales VLAN. Since these rules are based on Layer 3 information, an Engineering user could enter the network from a connection in the Sales department, and that user would still be contained in the Engineering VLAN.

## Traffic Filtering

Classification rules can also be used to filter out (discard) specific unwanted traffic. Filter criteria can include things such as broadcast routing protocols, specific IP addresses, or even applications such as HTTP or SMTP.

### OSPF/RIP Traffic Filtering



The figure above shows a common configuration in which a routed backbone is using both RIP and OSPF for its routing protocols. The network administrator does not want the multicast OSPF and broadcast RIP frames propagated to the end stations. The network is designed so that only end users are attached to the E7 devices.

To implement filtering in this scenario, a Layer 3 rule and a Layer 4 rule will be created.

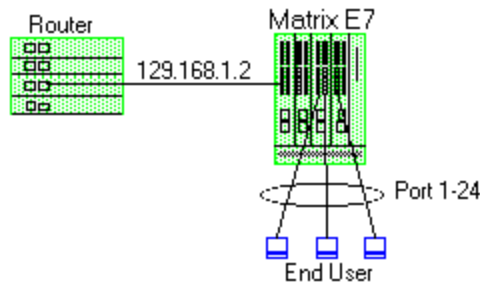
Rule 1 (Layer 3) - Any frame received with an IP Protocol Type of 89 (OSPF) will be discarded.

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

Based on this configuration, all RIP and OSPF frames will be filtered from the end users.

## Traffic Security

Traffic Security uses the same concepts as [Traffic Filtering](#). Imagine a scenario where network access is provided to a group of unknown users. There have been problems with these unknown users "hacking" into the router and altering the configuration. A simple classification rule can be put in place that will prevent these types of occurrences.

Router Traffic Security

In the figure above, the network components include a router and an E7 device. In this configuration end-users connect to the ports of the E7 device.

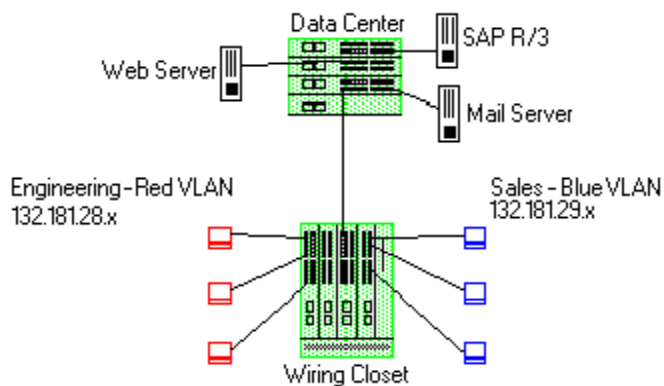
Since the end-users would never need to communicate directly to the router using the router's IP address, a Layer 3 IP classification rule will be used.

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

The end result is that any frames from a user trying to "hack" into the router will be discarded before ever reaching the router.

Traffic Prioritization

Classification rules can be used to specify that certain network applications receive the highest transmission priority. For example, a network administrator wants to assign priority to three network applications, SAP R/3, web traffic, and email, in that order.

Prioritization

To accomplish the prioritization goals in this example, there are two main steps required: creating the classification rules, and then configuring the priority-to-transmit queue mapping for the switch, if needed.

First, create one Layer 3 and two Layer 4 classification rules.

Rule 1, Layer 3 (SAP R/3) - All frames to or from the IP address of the SAP R/3 server will be tagged with a priority indicator of 7 (highest).

Rule 2, Layer 4 (Web) - All frames with a TCP port number of 80 (HTTP) will be tagged with a priority indicator of 5.

Rule 3, Layer 4 (email) - All frames with a TCP port number of 25 (SMTP) will be tagged with a priority indicator of 3.

**Note:** An IP address classification was selected for Rule 1 because it has been observed that SAP R/3 dynamically negotiates the TCP/UDP port used, so the port number selections vary from session to session. If this was not the case, a Layer 4 UDP classification could be used.

Then, configure the priority-to-transmit queue mappings. Each switch has default priority-to-transmit queue mappings. You can use these defaults or change the mappings using local management or NetSight Console. In addition, Policy Manager provides the ability to configure transmit queues as part of the Role-Based Rate Limits and Transmit Queue Configuration class of service mode. This functionality is available only on certain devices such as the S-Series and N-Series Gold and Platinum devices (refer to the NetSight Firmware Support tables for specific device/firmware rate limit support).

Based on the default priority-to-traffic queue mapping for an E7 device, the priorities assigned above will work out so that each frame classification type will be mapped to the desired traffic queue. This means that no user configuration of the priority-to-transmit queue mapping would be required.

With the classification rules described above, the network traffic would be prioritized as shown in the table below:

<b>Application</b>	<b>Classification Type</b>	<b>Desired Priority</b>	<b>Priority Value</b>	<b>E7 Traffic Queue</b>
SAP R/3	Bilateral IP	High	7	3
Web	TCP Port Number	Medium	5	2
Email	TCP Port Number	Low	3	1

## Classification Rules Precedence

When there is a role with multiple classification rules assigned to a port, the device determines which rule takes precedence based on an order of



precedence that is predefined in the device. Network administrators should have a comprehensive understanding of classification precedence, as it can significantly impact the operation of traffic classification rules. The [Device Support Tab \(Role\)](#) provides rule precedence information for each role. For additional information on rule precedence, see your device hardware documentation.

The device determines the order of precedence based on the classification types. If there are multiple rules with the same precedence, the more granular rule takes effect. Here are two examples of how this works:

- A rule that uses an IP address with a full mask has precedence over a rule with an IP address with a less granular mask. For example, an IP address of 1.1.1.1/32 would have precedence over an IP address of 1.1.1.1/24.
- A rule that uses an IP address with a port number has precedence over a rule with an IP address that does not. For example, an IP address of 1.1.1.1:80 would have precedence over an IP address of 1.1.1.1. This means that an IP Socket rule has a higher precedence than an IP Address rule.

The Precedence Table lists the order of precedence with 1 being the highest precedence, and 27 being the lowest.

<b>Classification Rule</b>	<b>Precedence</b>
MAC Address Source	1
MAC Address Destination	2
Application	3
IPX Network Source	4
IPX Network Destination	5
IPX Socket Source	6
IPX Socket Destination	7
IPX Class of Service	8
IPX Packet Type	9
IPv6 Address Source	10
IPv6 Address Destination	11
IPv6 Flow Label	12
IP Address Source	13
IP Address Destination	14
IP Fragment	15
IP UDP Port Source	16

Classification Rule	Precedence
IP UDP Port Destination	17
IP TCP Port Source	18
IP TCP Port Destination	19
ICMP	20
ICMPv6	21
IP Type of Service	22
IP Protocol Type	23
Ethertype	24
DSAP/SSAP	25
VLAN ID	26
Priority	27

---

**NOTES:** — The precedence of a rule based on a bilateral address match is determined frame by frame depending on whether the rule matches the destination or source address in the frame. A bilateral address rule which matches the source address has higher precedence than a rule which matches a destination address (or any other lower precedence rule).  
 — Device precedence lists show 31 entries and use a different numbering scheme than shown above.

---

### *Precedence Scenarios*

The following scenarios illustrate the classification rule precedence on S-Series and N-Series devices.

#### Scenario 1

A network administrator has defined two classification rules:

Rule 1- All frames with a UDP port number of 55 (ISI Graphic Language) are assigned to the Red VLAN.

Rule 2- All frames sourced from the 132.181.28.x subnet are assigned to the Blue VLAN.

If a frame is received with a source address of 132.181.28.99 and a UDP port number of 55, the frame will be assigned to the Blue VLAN because as shown in the [Precedence Table](#), an IP Address rule takes precedence over a UDP rule.

## Scenario 2

A network administrator defines two classification rules:

Rule 1- All frames with an IP ToS value of AA are assigned a priority of 7.

Rule 2- All frames with a TCP port number of 80 (HTTP) are assigned a priority of 3.

If a frame is received with a ToS value of AA and a TCP port number of 80, the frame will be assigned a priority of 3, because as shown in the [Precedence Table](#), TCP port number classifications take precedence over IP ToS classifications.

---

## Related Information

For information on related tasks:

- [How to Create or Modify a Rule](#)
- [How to Define Traffic Descriptions](#)

# Getting Started with Class of Service

---

This Help topic provides an overview of Policy Manager's class of service (CoS) functionality, including information about defining rate limits and configuring transmit queues.

After you have read this topic, look at an example of how a network administrator might use CoS to configure VoIP traffic with appropriate priority, ToS, queue treatment, and flood control by clicking on the link: [Class of Service Example](#).

This guide includes the following information:

- [Class of Service Overview](#)
- [Rate Limits](#)
- [Transmit Queues](#)
- [Flood Control](#)

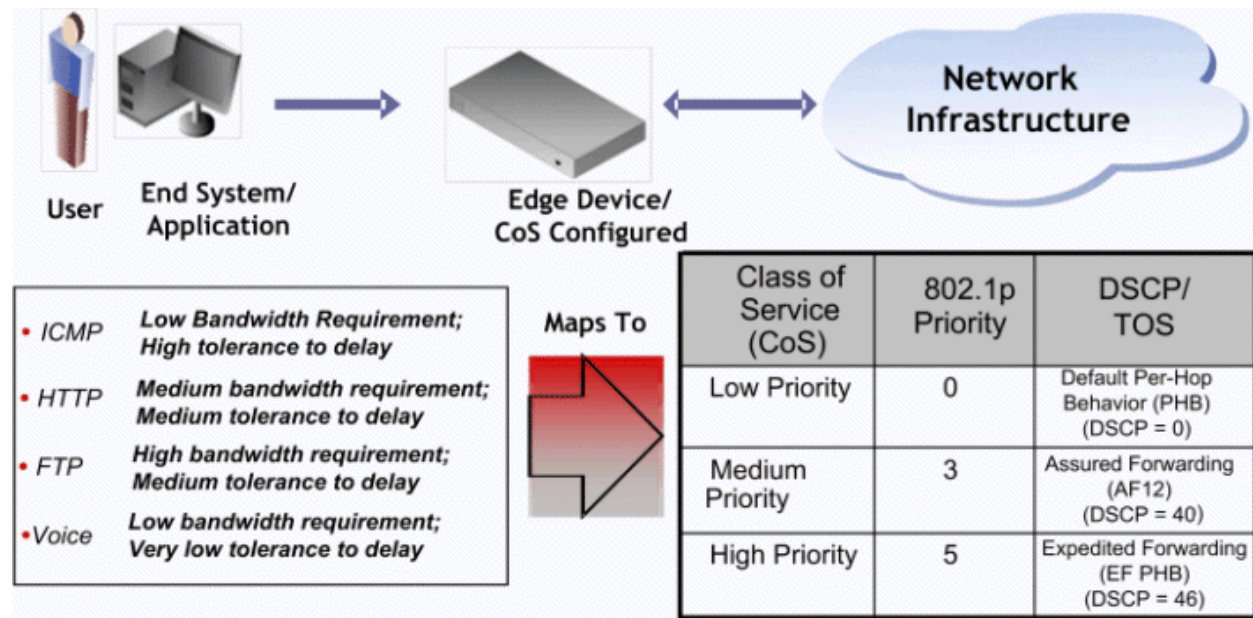
## Class of Service Overview

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

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

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

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



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

## Implementing CoS

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

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

## Configuring CoS

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

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

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

To view and configure CoS, open the [Class of Service Configuration window](#) from the Policy Manager Edit menu. You will see that it is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS/DSCP, drop precedence, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service (user-defined CoS).

## Rate Limits

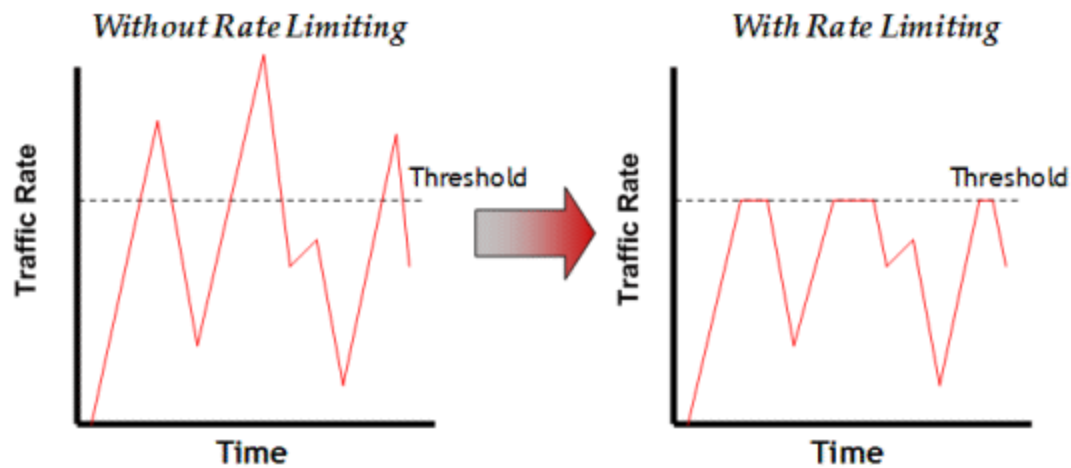
Rate limits are one component of a Policy Manager class of service. They are used to control the transmit rate at which traffic enters and exits ports in your network. All traffic mapped to a Class of Service on a given port will share the bandwidth specified by the rate limit.

For instructions on how to configure rate limits, see [How to Define Rate Limits](#).

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

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

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



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

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

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

## Transmit Queues

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

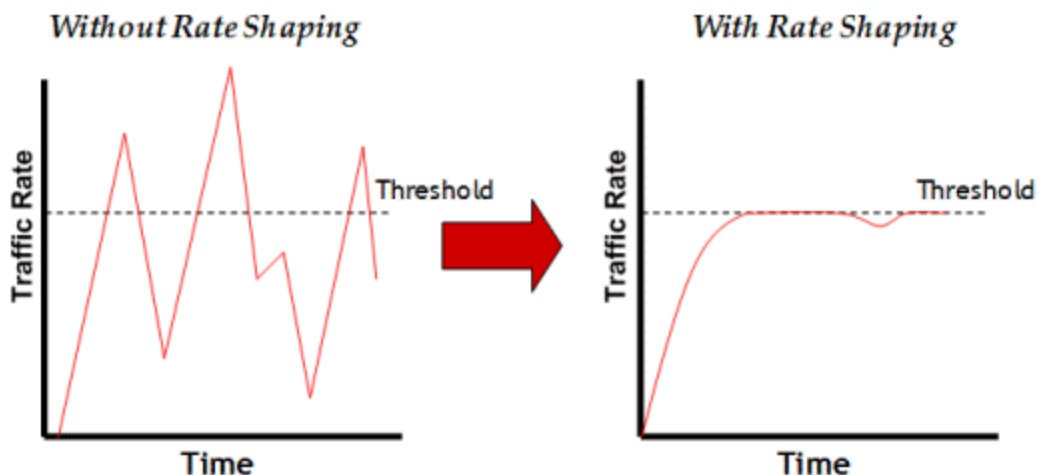
For instructions on how to configure transmit queues, see [How to Configure Transmit Queues](#).

There are three components to transmit queue configuration:

- Transmit Queue Configuration allows you to set the transmit queue associated with the class of service.
- Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of that transmit queue.
- Bandwidth Configuration allows you to specify how the traffic in each transmit queue is serviced as it egresses the port.

The transmit queue configuration will remain on the port only as long as the role using the configuration is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is smoothed out when it goes above the assigned threshold when rate shaping is applied.



Rate shaping retains excess packets in a queue and then schedules these packets for later transmission over time. Therefore, the packet output rate is smoothed and bursts in transmission are not propagated as seen with rate limiting.

Rate shaping can be used for the following reasons:

- to control bandwidth
- to offer differing levels of service
- to avoid traffic congestion on other network links by removing the bursty property of traffic that can lead to discarded packets



Policy Manager class of service also provides the ability to create transmit queue shaper port groups that allow you to isolate certain kinds of sensitive network traffic so that you can vary the bandwidth of the shape for that single queue. For more information on transmit queue port groups, see [Creating Class of Service Port Groups](#).

## Flood Control

Flood control provides rate limiting capabilities to individual Class of Service to allow certain types of flooded traffic to be dropped. When enabled, incoming traffic is monitored over one second intervals. Traffic is identified using the following configuration types:

- unknown - unicast
- broadcast
- multicast

A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then allowed to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similar to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, once Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

For instructions on how to configure flood controls, see [How to Configure Flood Control](#).

---

### Related Information

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

## Class of Service Example

This Help topic provides an example of how class of service (Cos) can be configured on a network to manage bandwidth requirements of network traffic. Before you look at this example, it is recommended that you read [Getting Started with Class of Service](#).

In this example, an organization's network administrator needs to assure that VoIP traffic, both originating in and transiting a network of edge switches and a core router, is configured with appropriate priority, ToS, and queue treatment. We will also rate limit the VoIP traffic at the edge to 1 Mb/s to guard against DOS attacks, VoIP traffic into the core at 25 Mb/s, and H.323 call setup at 5 PPS. Data traffic retains the default configuration.

This example assumes CEP authentication using H.323 for VoIP. For networks that do not authenticate VoIP end point with CEP H.323 authentication, the VoIP policy will need to be adjusted accordingly. For instance, SIP uses UDP port 5060, not the TCP port 1720.

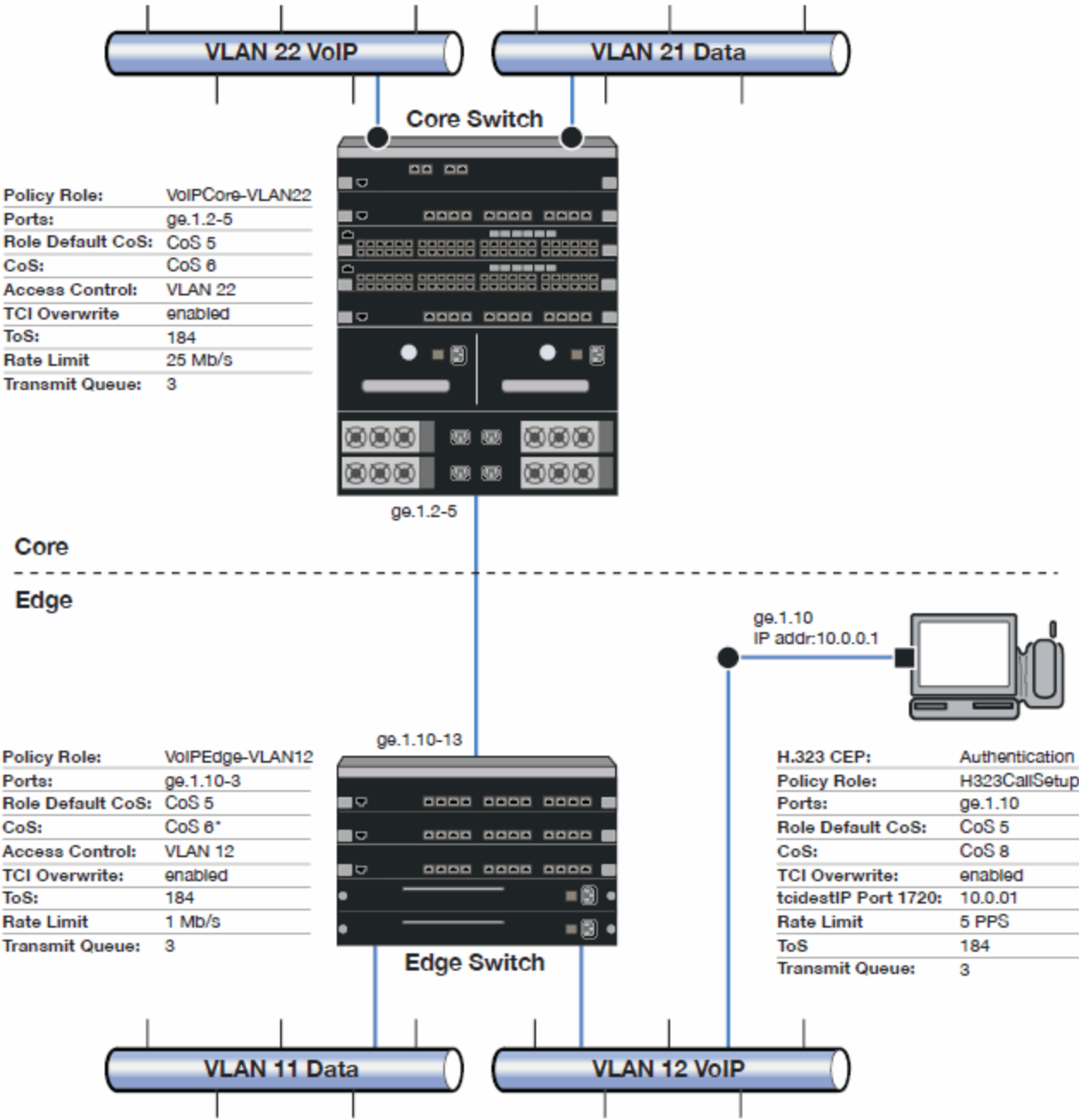
To simplify the discussion of the configuration process, this example is limited to the VoIP configuration context. The following table provides a set of sample values for priority, inbound rate limit (IRL), and transmit queue across a number of real world traffic types. This table can be used as an aid in thinking about how you might want to apply CoS across your network. Note that Scavenger class is traffic that should be treated as less than best effort: external web traffic, for instance.

CoS Name	CoS Index	Priority	IRL		Transmit Queue					
					Queue #		Shaping		Bandwidth	
			Edge	Core	Edge	Core	Edge	Core	Edge	Core
Scavenger (Static)	0	0	15 Mb/s		0	0	10%		5%	5%
Best Effort (Static)	1	1								
Bulk Data (Static)	2	2			1	1	80%		45%	45%
Critical Data (Static)	3	3								
Network Control (Static)	4	4	40 PPS	1 Mb/s	2	2	1 Mb/s		25%	25%
Network Mgmt (Static)	5	5	2 Mb/s							
RTP/Voice/Video (Static)	6	6	1 Mb/s	25 Mb/s	3	3			25%	25%
High Priority (Static)	7	7								
VoIP Call Setup	8	7	5 PPS		3	3			25%	25%

The following figure displays the network setup for this example configuration, with the desired Profile/CoS summary for each network device. Each device is

configured with VoIP and Data VLANs. Each VoIP VLAN contains four 1 gigabit interfaces for each device.

CoS VoIP Configuration Example



Edge and Core port groups in the RTP/Voice/Video (Static) CoS provide for the difference in rate limiting needs between the end user and aggregation devices. A VoIP Call Setup CoS provides rate limiting for the setup aspect of the VoIP call.

The Edge, Core, and H.323 Call Setup roles are configured with TCI Overwrite, default CoS 5 (best default priority for voice and video), and default access control that contains traffic to the appropriate VLAN.

Use Policy Manager to configure the policy roles and related services using the following instructions. For more information, see [How to Create a Class of Service](#) and [How to Define Rate Limits](#).

## Configure the Classes of Service

Use the Class of Service Configuration window to configure the static RTP/Voice/Video CoS with the appropriate edge and core rate limits, and create a new CoS for the call setup rate limits.

1. For the static RTP/Voice/Video CoS (CoS Index 6):
  - a. Set the ToS to B8.
  - b. Create two new Inbound RL port groups called Edge and Core.
  - c. Set the Edge port group rate limit to 1 Mb/s and the Core port group rate limit to 25 Mb/s. (You may need to first create these rate limits.)
  - d. Add the appropriate ports to each port group.
2. Create a new class of service and name it VoIP Call Setup (CoS Index 8).
  - a. Set the rate limit to 5 PPS for all port groups. (You may need to first create this rate limit.)
  - b. Set the ToS to B8.

## Create the VoIP Core Role

For the core router, create a policy role for VoIP Core. VoIP Core policy deals with packets transiting the core network using VoIP VLAN 22.

1. Name the role VoIPCore √VLAN22.
2. Enable TCI overwrite so that ToS will be rewritten for this role.
3. Set the default access control action to Contain to VLAN 22.
4. Set default Class of Service to CoS Index 5.

### *Create a VoIP Core Service*

1. Name the service VoIPCore.
2. Add the service to the VoIPCore VLAN22 role.

### *Create a Rule*

1. Create a Layer 2 traffic classification rule for VLAN ID 22 within the VoIPCore service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

## **Creating the VoIP Edge Role**

For the edge switches, create a policy role for VoIP Edge. VoIP Edge policy deals with packets transiting the edge network using VoIP VLAN 12.

1. Name the role VoIPEdge VLAN12.
2. Enable TCI overwrite so that ToS will be rewritten for this role.
3. Set the default access control action to Contain to VLAN 12.
4. Set default Class of Service to CoS Index 5.

### *Create a VoIP Edge Service*

1. Name the service VoIPEdge.
2. Add the service to the VoIPEdge VLAN12 role.

### *Create a Rule*

1. Create a Layer 2 traffic classification rule for VLAN ID 12 within the VoIPEdge service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

## **Creating the H.323 Call Setup Role**

The H.323 Call Setup role deals with the call setup traffic for VoIP H.323 authenticated users directly attached to the switch using link ge.1.10.

1. Name the role H323CallSetup.
2. Enable TCI overwrite so that ToS will be rewritten for this policy.
3. Set default Class of Service to CoS Index 5.

### *Create a H.323 Call Setup Service*

1. Name the service H323CallSetup.
2. Add the service to the H323CallSetup role.

### *Create a Rule*

Create a Layer 4 traffic classification rule as follows:

1. Traffic Classification Type: IP TCP Port Destination
2. Enter in Single Value field: 1720 (TCP Port ID).
3. For IP TCP Port Destination value: 10.0.0.1 with a mask of 255.255.255.255.
4. Assign the new VoIP Call Setup CoS (CoS Index 8) as the Class of Service action for the rule.

## **Apply the Roles to Network Devices**

Once you have created your roles, you must apply them to the network devices as follows:

### **Core Router**

Apply the VoIPCore vLAN22 role to ports ge.1.2 5.

### **Edge Switch**

Apply the VoIPEdge vLAN12 role to ports ge.1.10 13.

Apply the H323CallSetup role to port ge.1.10

## How to Create a Class of Service

---

Policy Manager lets you define classes of service (CoS) that can include one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

When you install Policy Manager, the Class of Service Configuration window (available from the Policy Manager Edit menu) is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS/DSCP, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service.

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

It is recommended that you read [Getting Started with Class of Service](#) before creating your classes of service.

Instructions on:

- [Creating a Class of Service](#)
- [Creating Class of Service Port Groups](#)
- [Deleting a Class of Service](#)

### Creating a Class of Service

The basic components for a class of service include an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

Use the following instructions to create a new class of service using the [Class of Service Configuration window](#).

1. Open the Class of Service Configuration window (available from the Policy Manager Edit menu).
2. Click the **Create** button and select **Create Class of Service** from the menu.
3. In the Name field, enter the name for the class of service.

4. If the class of service includes an 802.1p priority, select the checkbox and use the drop-down list to choose the priority (0-7 with 7 being the highest priority).
5. If desired, select the ToS/DSCP Marking option to associate an IP ToS (Type of Service) or DSCP (Diffserv Codepoint) value with the class of service (see [IP Type of Service](#) for more information). You can either enter a value in the **Value Ox** text box, or click **Select** to open the [ToS/DSCP Configuration window](#), where you can automatically configure a ToS (Type of Service) or DSCP (Diffserv Codepoint) value.
6. If desired, specify a Drop Precedence. The Drop Precedence is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence will dictate the internal priority (within the MAC chip) that will be used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.
7. Use the drop-down menu to select a transmit queue for the class of service. If you would like to select a different transmit queue for each port type, select the "Q/Port Type" option. Then, when you click **Apply** or **OK**, you will see a window where you can specify a different transmit queue for each port type.
8. If desired, use the Rate Limit Configuration section to select a port inbound and outbound rate limit to associate with the class of service. Click **Create** on the drop-down menu to open the [Create Rate Limit window](#) where you can create a new rate limit. The rate limit you select here will be applied to all IRL/ORL [port groups](#). To configure different rates for each port group, use the Class of Service Configuration window.
9. If you have ExtremeWireless Wireless Controllers on your network, you will see an option to select inbound and outbound user rate limits to associate with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for wireless controllers.
10. Click **OK**. The class of service is created and is listed in the Class of Service Configuration table.



11. Click the **Save** button on the Policy Manager toolbar to save your new Class of Service to the Policy Manager database.

After a class of service has been created, you can double-click in the Class of Service Configuration table to modify its characteristics, if necessary.

## Creating Class of Service Port Groups

Policy Manager provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For example you might want to create a class of service where your edge ports would receive one rate limit while your core ports would receive a different rate limit. With port groups, you can create a single class of service that assigns a different rate limit to each group.

It also provides the ability to create transmit queue shaper port groups that allow you to isolate certain kinds of sensitive network traffic so that you can give it a high transmit queue priority. For example, ports on a router might be grouped together and configured with a specific rate shaping parameter. A transmit queue port group may contain multiple port queue types (for example, 4-queue ports and 16-queue ports) depending on the type of devices on your network.

Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

The following instructions are for creating new port groups for an existing class of service.

1. Open the [Class of Service Configuration window](#) (available from the Policy Manager Edit menu).
2. Click the **Create** button and select the menu option to create the desired group type: rate limit (RL) port group or transmit queue (TxQ) shaper port group. You can also right-click on the table column heading to see a menu option for creating a group.
3. The Create CoS Port Group window opens. Enter a name for the port group. Use the **Also Create** option if you want to create multiple port group types with this same name.
4. The new port group appears in the Class of Service Configuration table under the appropriate port group type.
5. Right-click on the new port group heading and select **Add/Remove Ports**.

6. The [Add/Remove Ports window](#) opens with the ports in the Default port group displayed in the left panel. Add ports to the new port group by selecting the ports in the left-panel, then selecting the port group in the right panel, and clicking **Add**. Click **OK** to close the window.
7. To configure different rates for each port group, double-click in the column under the port group to set or change a rate for each port group.
8. Click **Save** on the toolbar.

## Deleting a Class of Service

1. Open the [Class of Service Configuration window](#) (available from the Policy Manager Edit menu).
  2. Right-click the class of service you want to remove, and select **Delete**.
  3. Click **OK** to confirm that you want the class of service removed.
  4. Click **Save** on the toolbar.
- 

## Related Information

For information on related tasks:

- [Getting Started with Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

For information on related windows:

- [Create Class of Service Window](#)
- [General Tab \(Class of Service\)](#)

## How to Configure Transmit Queues

---

Policy Manager allows you to configure transmit queues as a component of a [class of service](#) (CoS).

There are three transmit queue configuration capabilities:

- Transmit Queue Configuration - Allows you to set the transmit queue associated with the class of service.
- TxQ Shaper - Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of a transmit queue.
- Bandwidth Configuration - Allows you to specify how the traffic in each transmit queue is serviced as it egresses the port.

These three capabilities are configured in the [Class of Service Configuration window](#) available from the Policy Manager Edit menu.

For more information, see the section on transmit queues in [Getting Started with Class of Service](#).

Instructions on:

- [Transmit Queue Configuration](#)
  - [Transmit Queue Bandwidth Configuration](#)
  - [Setting the Arbiter Mode](#)
- [Transmit Queue Rate Shapers](#)

### Transmit Queue Configuration

Transmit queues represent the hardware resources for each port that are used in scheduling packets for egressing the device. By default, the static classes of service 0-7 map to transmit queues 0-7. The actual transmit queue number may vary depending on the number of queues supported by the port.

The Queue column in the Class of Service Configuration window displays the actual transmit queues associated with the class of service for each port type. Double-click in the column to see a drop-down menu where you can select a new transmit queue for all port types, or select a different transmit queue for each individual port type.

**TIP:** For more detailed information, refer to the tooltip that appears when you hover the cursor over the Queue column.

---

### *Transmit Queue Bandwidth Configuration*

The transmit queue arbiter mode is the method used to determine how traffic in each transmit queue is serviced. It is based on a percentage or weight (called a "slice") given to each queue.

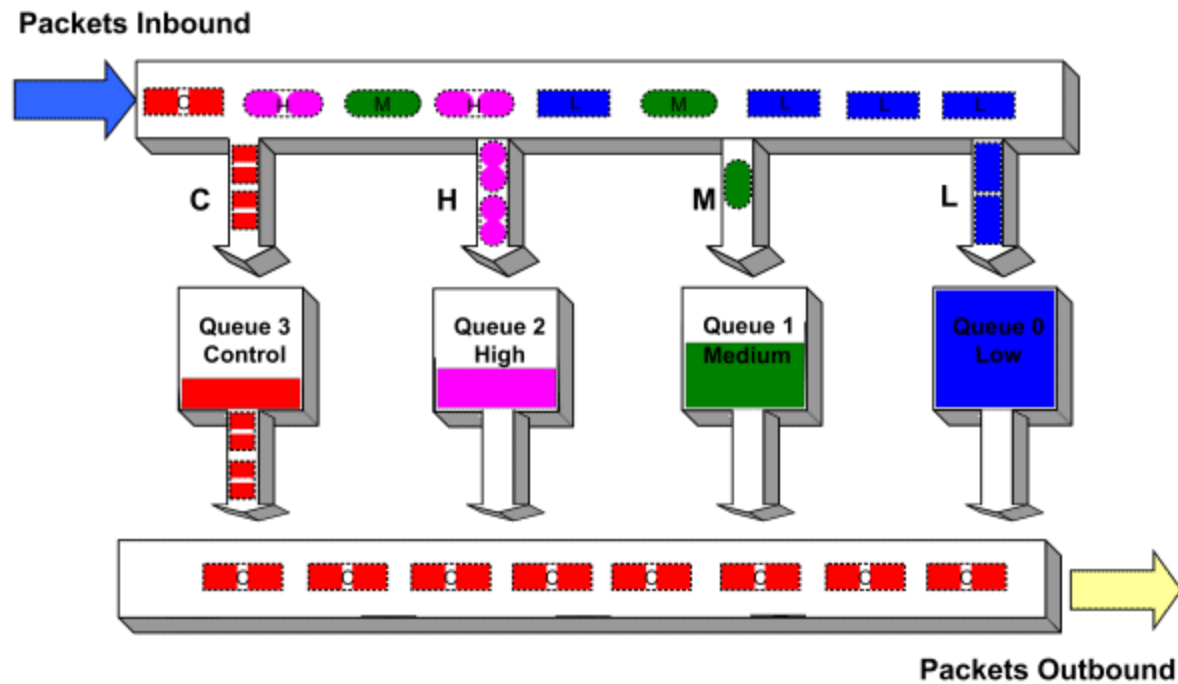
There are three types of arbiter mode: strict priority mode, weighted fair mode, and Enhanced Transmission Selection mode. Each of these modes handles egress traffic differently. In addition, some devices support low latency queues (LLQ) which also impact how egress traffic is handled.

#### **Strict Mode**

By default, ports are set to Strict mode, which means that the highest priority queue (the highest numbered queue) is set to 100%. In Strict mode, queues are serviced by numerical priority from the highest numbered queue to the lowest, and all frames in the highest priority queue will be transmitted before the frames in lower priority queues.

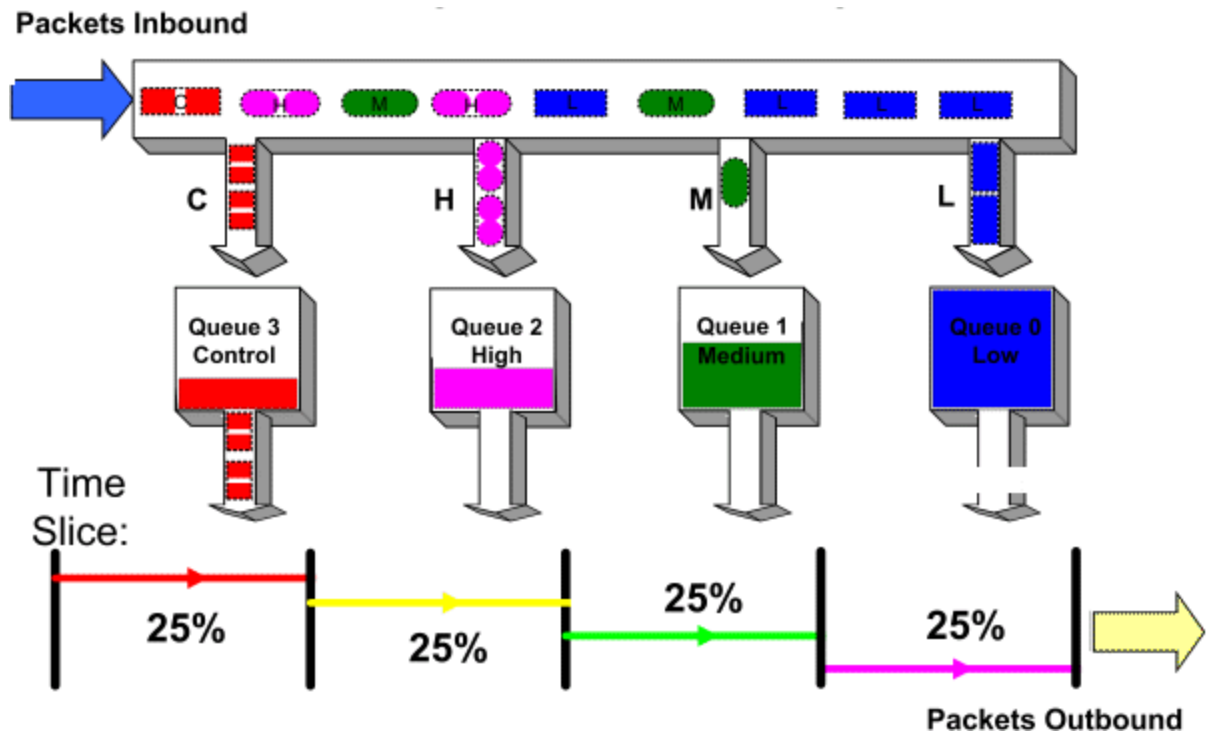
Strict priority queuing assures that the highest priority queue with any packets in it will get 100 percent of the bandwidth available. This is particularly useful for one or more priority levels with low bandwidth and low tolerance for delay. The problem with strict priority queuing is that if the higher level queues never fully empty, lower level queues can be starved of bandwidth.

Strict priority queuing is depicted in the following figure. Inbound packets enter on the upper left and proceed to the appropriate queue based upon the TxQ configuration in the CoS. Outbound packets exit the queues on the lower right. In the figure, only queue 3 packets are forwarded, and this will be true until queue 3 is completely empty. Queue 2 packets will then be forwarded. Queue 1 packets will only forward if both queue 2 and queue 3 are empty. Queue 0 packets will only forward if all other queues are empty.

Strict Priority Queuing**Weighted Fair Mode**

You can change the arbiter mode to Weighted Fair Queuing, which lets you adjust the slice percentage for each queue and prevent a lower priority queue from being starved. Queues are serviced according to the percentage or weight you assign to each queue. This prevents a lower priority queue from being starved. Percentages must add up to 100%. (Configuring 100% for the highest priority queue sets the port to Strict mode.)

The following figure depicts how weighted fair queuing works. Inbound packets enter on the upper left of the box and proceed to the appropriate priority queue. Outbound packets exit the queues on the lower right. Queue 3 has access to its percentage of time slices so long as there are packets in the queue. Then queue 2 has access to its percentage of time slices, and so on round robin.

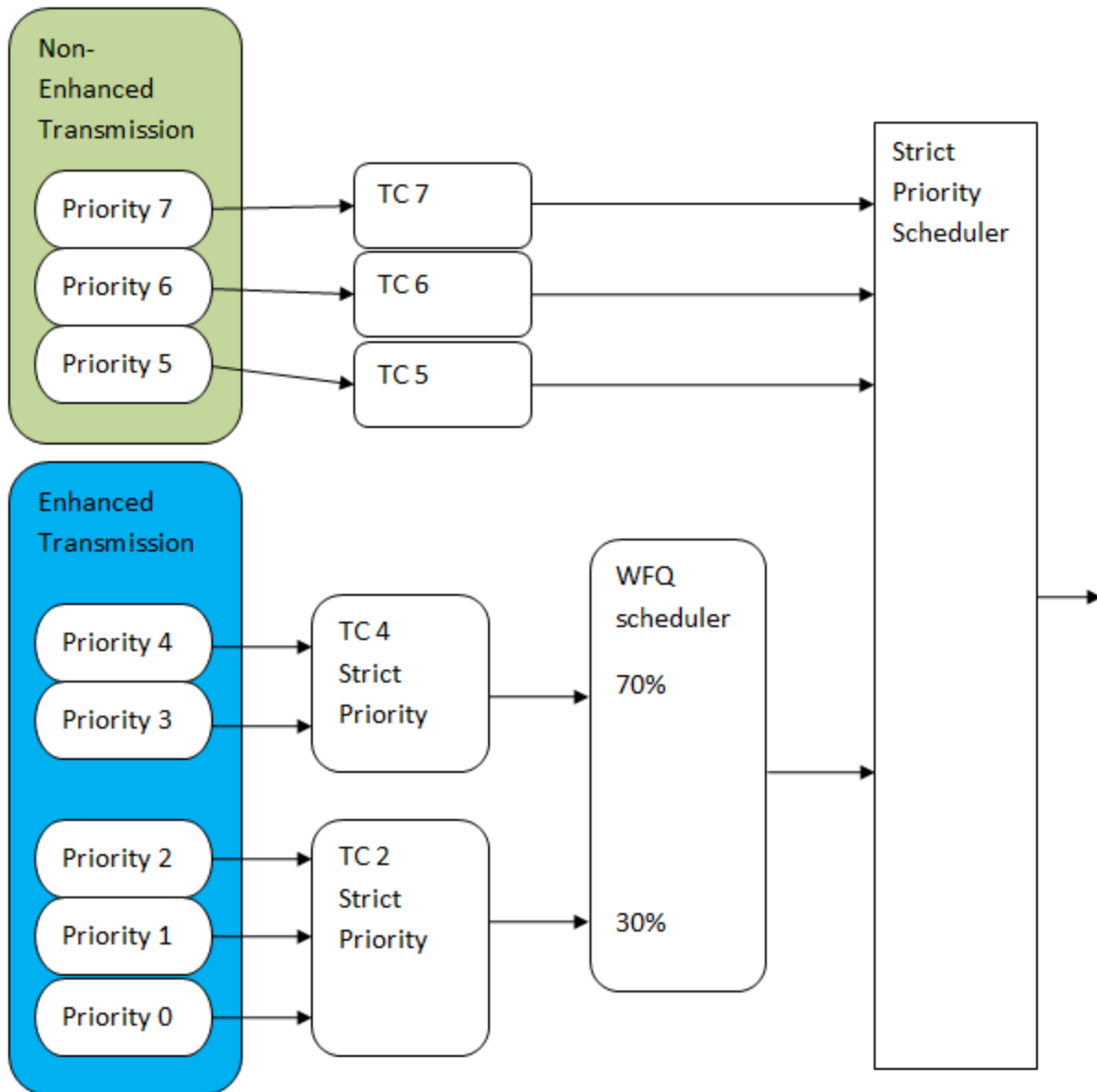
Weighted Fair Queuing

Weighted fair queuing assures that each queue will get at least the configured percentage of bandwidth time slices. The value of weighted fair queuing is in its assurance that no queue is starved for bandwidth. The downside of weighted fair queuing is that packets in a high priority queue, with low tolerance for delay, will wait until all other queues have used the time slices available to them before forwarding. So weighted fair queuing would not be appropriate for applications with high sensitivity to delay or jitter, such as VoIP.

### Enhanced Transmission Selection Mode

You can change the arbiter mode to Enhanced Transmission Selection (ETS), which allows you to designate 2 or more transmit queues as ETS queues. The ETS queues are then assigned bandwidth allocation with the sum of the ETS queues bandwidth equaling 100%. The scheduler will then service all non-ETS queues first using strict priority. The remaining bandwidth is then distributed based on the allocation that was defined for each of the ETS queues. The priorities within an ETS queue are serviced by strict priority.

The following diagram depicts how ETS works. Priorities 7, 6, and 5 are not part of ETS and will be serviced first. Once these queues have been processed, the remaining bandwidth is then allocated to ETS queues 3 and 0. The ETC queues are then assigned 70 and 30 % bandwidth.

Enhanced Transmission Selection

The Traffic Class (TC) identifiers are first assigned from the lowest to highest based on the priority of the TxQs which the 802.11D maps. This is determined by the Class of Service (CoS) configuration. If the 802.11D priority maps to a customer TxQ (1-8) which is configured for ETS, all priorities which map to the same traffic class groups are assigned the highest priority TC identifier.

---

**NOTE:** Low Latency Queuing (LLQ) ports may not be assigned to ETS groups.

---

## Low Latency Queuing

Extreme Networks K-Series, S-Series, and N-Series devices (with firmware version 7.0.1) support Low Latency Queuing (LLQ) also known as Hybrid queuing. The two highest queues (highest priority) and the lowest queue (lowest priority) will always be designated as LLQ queues. With LLQ, your queuing configuration might look something like:

- 1) Voice (low-latency, high priority, strict queue)
- 2) Video (low-latency, high priority, strict queue)
- 3) Traditional data traffic such as TCP (weighted fair queuing and rate shaping)
- 4) Guest traffic or internet traffic (low-latency, low priority, strict queue)

Note that Strict or Weighted Fair Queuing are still used to configure the slice distribution on the non low-latency queues carrying traditional data traffic.

---

**NOTE:** N-Series Gold devices do not support arbiter mode and slice percentage configuration. Ports on these devices that are included in the port group will ignore these settings.

---

## *Setting the Arbiter Mode*

To specify the arbiter mode:

1. In the Class of Service Configuration window (available from the Policy Manager Edit menu), double-click in the Transmit Queue Bandwidth column. The [Edit Bandwidth Configuration Window](#) window opens.
2. Select the desired transmit queue Arbiter Mode: Strict, Weighted Fair Queuing, or Enhanced Transmission Selection. If you want to specify an arbiter mode independently for each port type (for example, 11 Queue Ports or 16 Queue ports), select Use Per-Port Type Arbiter Mode.
3. If you have selected Weighted Fair Queuing, click the **Edit** button to open the [Slice Percentages Window](#). Set the desired slice configuration and click **OK**.
4. Click **OK** to close the Edit Bandwidth Configuration window.
5. Click **Save** on the toolbar to save the configuration change to the database.

## Transmit Queue Rate Shapers

Rate shapers let you pace the rate at which traffic is transmitted out of a transmit queue. Packets received above the configured rate are buffered rather than dropped. Only when the buffer fills are packets dropped.



The following steps describe how to configure rate shapers in Policy Manager:

1. In the Class of Service Configuration window (available from the Policy Manager Edit menu), select the class of service where you want to configure the transmit queue.
2. Double-click on the selected line below the TxQ Shaper column and select the desired rate shaper from the drop-down menu. For information on how to create a new rate, see the [Create Rate Limit/Shaper Window](#) Help topic.
3. Click **Save** on the toolbar to save the configuration change to the database.

For more information, see the section on transmit queues in [Getting Started with Class of Service](#).

---

**NOTE:** A rate shaper is associated to a specific transmit queue, not a CoS. This means that the 1) you should select the queue you want to use for a CoS first, then set the shaper and 2) all CoS using that queue will use the same rate shaper.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)

## How to Configure Flood Control

---

Flood Control provides rate limiting capabilities to CoS to allow certain types of flooded traffic to be dropped. The flood control traffic types are:

- unknown - unicast
- broadcast
- multicast

When Flood Control is enabled, incoming traffic is monitored over one second intervals. A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then allowed to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similarly to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, once Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

### How to Display Flood Control Port Groups on the CoS Configuration Window

1. From the Edit menu, select **Class of Service Configuration**. The CoS Configuration window opens.
2. Verify that Flood Control is set to be managed by Policy Manager for this domain by ensuring that either **All Components** or **Flood Control** are selected in the Domain Managed CoS Components menu.
3. To easily navigate to Flood Control components of CoS, click the **Table Display Filter** button, and select **Flood Control**. A Flood Control column displays for each CoS. Each column will either display the configured rate limit or None, if no rate has been defined for that portion of Flood Control. This will remove the other sections of Class of Service, making the table easier to read.

### How to Create a Flood Control Port Group

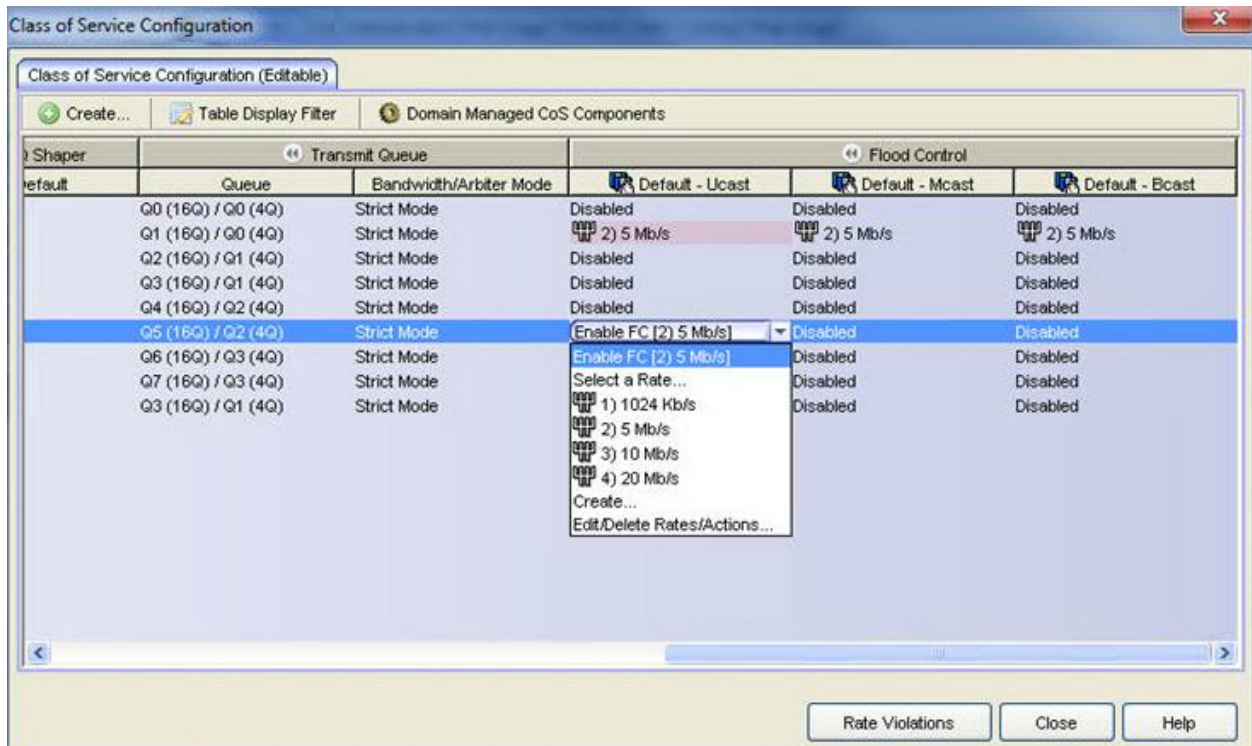
1. From the Edit menu, select **Class of Service Configuration**. The CoS Configuration window opens.

2. Click the **Create** button or right-click the Flood Control column header, and select Create Flood Control Port Group.
3. In the Create CoS Port Group dialog, under Create FLD Port Group, enter a name for the Flood Control Port Group. In addition to CoS, you can also create a port group for IRL, ORL, and TXS by selecting each individual group from the drop-down menu. A New Flood Control item is added to the CoS Configuration Window.

### How to Enable/Disable Flood Control for a CoS

Flood Control Rate Limits are shared across all CoS. Once a Flood Control rate has been enabled on at least one CoS, that is the rate specified for all Flood Control enabled CoS.

1. Double-click the column for the desired Flood Control broadcast traffic type Ucast (unicast), Mcast (multicast), or Bcast (broadcast), and select a rate from the drop-down menu.
2. Select a rate that has been created or create a new one. If Flood Control is enabled on an existing CoS, the Flood Control can be enabled/disabled for this CoS by selecting the **Enable/Disable** Flood Control option from the drop-down menu.



### How to Add/Remove Ports to Flood Control Port Groups

1. From the Edit menu, select **Class of Service Configuration**. The CoS Configuration window opens.
  2. Right-click the Flood Control column header, and select Add/remove Ports.
  3. In the Add/Remove Ports dialog, select the Port Groups from the right column and click **Remove**. You can also delete multiple Port Groups by clicking **Remove All**.
- 

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)
- [Class of Service Configuration Window](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)
- [General Tab \(Class of Service\)](#)

## How to Define Rate Limits

---

Policy Manager allows you to create and define [rate limits](#) as components of a [class of service](#). Rate limits are used to control the transmit rate at which traffic enters and exits ports in your network.

Policy Manager uses role-based rate limits that are tied directly to roles and rules, and are written to a device when the role/rule is enforced.

---

**Note:** Policy Manager also supports priority-based rate limits for use with legacy devices. See How to Configure [How to Define Priority-Based Rate Limits](#) for more information. Refer to the NetSight Firmware Support tables to determine which type of rate limit a specific device/firmware supports.

---

Instructions on:

- [Defining Rate Limits](#)
- [Removing a Rate Limit](#)

### Defining Rate Limits

Rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. When role-based rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

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

You can create a rate limit at the same time that you assign a rate limit to a CoS for a specific port group.

1. Open the Class of Service Configuration window (available from the Policy Manager Edit menu).
2. In the table, select the desired CoS and then double-click on that row under an Inbound RL port group (the Default group or a group you created) to display a drop-down menu. Select **Create** to open the Create Rate Limit/Shaper window.

3. Fill out the [Create Rate Limit/Shaper window](#):
  - a. Specify the desired rate limit.
  - b. Select the action you would like performed if the rate limit is exceeded:
    - Generate System Log on Rate Violation - a syslog message is generated when the rate limit is first exceeded.
    - Generate Audit Trap on Rate Violation - an audit trap is generated when the rate limit is first exceeded.
    - Disable Port on Rate Violation - the port is disabled when the rate limit is first exceeded.

---

**NOTE:** N-Series Gold devices do not support rate limit notification.

---

- c. Click **OK**.

The rate limit will appear in the CoS Configuration table mapped to the CoS.

Role-based rate limits are written to your devices when you enforce the role that includes them.

## Removing a Rate Limit

Rate limits remain on a port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role. To remove a rate limit, you must delete it from Policy Manager and then enforce. This will remove the rate limit from any roles it was associated with.

1. Open the Class of Service Configuration window (available from the Policy Manager Edit menu).
2. In the table, double-click on the rate you want to remove.
3. Select **Edit/Delete Rates/Actions** from the drop-down menu.
4. In the [Edit Rate Limit/Shaper\(s\) window](#) select the **Delete this Rate Limit/Shaper** checkbox and click **OK**.
5. Enforce.

---

**NOTE:** If you simply select **None** from the drop-down menu, it will un-map the rate from the class of service but it will not remove the rate limit.

---

## Related Information

For information on related concepts:

- [Rate Limits](#)

For information on related tasks:

- [How to Create a Class of Service](#)

For information on related windows:

- [Create Rate Limit Window](#)
- [General Tab \(Rate Limit\)](#)

## Advanced Rate Limiting by Port Type

---

The Policy Manager class of service feature provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For instructions on creating a port group, see [Creating Class of Service Port Groups](#).

This Help topic provides information about an advanced port group feature that lets you specify different rate limits for the different port types contained in a port group: 8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit port types.

---

**NOTE:** This feature requires CoS Advanced mode to be enabled.

---

After you have created your port groups, you can use the [CoS to rate limit mappings tab](#) to configure rate limit index mappings for each group. These mappings map a logical rate limit index to an actual physical rate limit created in Policy Manager. For each class of service, you can select one mapping index that gives you the desired physical rate limit for each port group (see the [Index Numbers](#) section of the CoS General tab for more information on CoS Index Numbers).

Policy Manager supports a maximum of 100 logical rate limit indexes and each rate limit port group lets you map all 100 indexes. For 8-rate limit, 32-rate limit, and 64-rate limit ports, this means that the number of logical indexes might be greater than the actual number of rate limits the port supports. The port group can map 100 logical rate limit indexes, but they can only be mapped to a maximum of 8, 32, or 64 different physical rate limits on those ports.

For example, let's say you want to have 25 rate limits for 25 different COS. You would need to define the behavior for the 8-rate port type, since once you get to the 9th rate, you would have no more resources available for the remaining rates (9-25). You would either need to share some of the same resources, or not rate limit with the remaining rates.

The maximum supported indexes for a device is based on the largest number of rates supported for that device. On devices supporting a maximum of 8 rate limits, indexes 0-7 are supported. On devices supporting a maximum of 32 rate limits, indexes 0-31 are supported. On devices supporting 64 rate limits, IRL indexes 0-63 are supported. If a rate limit port group maps indexes greater than the supported value, they are ignored during Enforce (indicated in the Class of Service > Rate Limit Mappings tables of Enforce Preview)



Instructions on:

- [Configuring Rate Limit Mappings](#)
- [Associating Rate Limits with a Class of Service](#)

## Configuring Rate Limit Mappings

Use the following instructions configure rate limit mappings for a port group.

1. Open the [Class of Service Configuration window](#) (available from the Policy Manager Edit menu).
2. From the **Domain Managed CoS Components** menu, select the **Show all CoS Components in Tree (Advanced Mode)** option to display the CoS tree in the left panel.
3. Expand the folders to select the rate limit port group in the left-panel tree.
4. Select the right-panel [CoS - Rate Limit Mappings tab](#).
5. Click **Add/Edit** to open the [Add/Edit CoS to Rate Limit Mappings window](#).
6. In the window, specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.
7. Use the drop-down list to select a rate limit to map to the index. Select **Create** to open the [Create Rate Limit window](#) where you can define a new rate limit, if needed.
8. The port type options allow you to create a mapping for all port types at once, or create a mapping just for specific port types.
9. The CoS IRL/ORL Index Usage table displays the IRL/ORL indexes being used by each class of service. You can use this table to determine which classes of service will use the rate limit, depending on whether the class of service has been mapped to an IRL or ORL.
10. Use the **Apply** button to map all your indexes without having to re-open the window. Click **OK** to close the window. The Mappings tab will display your index to rate limit mapping configuration.

## Associating Rate Limits with a Class of Service

After you have configured the rate limit mappings for a port group, you can associate a rate limit mapping index with a class of service.

1. Open the [Class of Service Configuration window](#) (available from the Policy Manager Edit menu).
  2. From the **Domain Managed CoS Components** menu, select the **Show all CoS Components in Tree (Advanced Mode)** option to display the CoS tree in the left panel.
  3. Select the class of service in the left-panel tree. (If you have not created the class of service, see [How to Create a Class of Service](#).)
  4. At the bottom of the right-panel General tab, click the button next to the IRL or ORL index that you want to configure. The Inbound/Outbound Rate Limits Selection View opens.
  5. This window lists all the currently mapped rate limits, organized by index number for each existing port type and group. Selecting one index number automatically includes all the rate limits configured for that index number. To configure new mappings for the CoS, you can first select an index that is not currently mapped, then create the mappings as described in [Configuring Rate Limit Mappings](#) above. Click **OK**.
  6. Once you have selected the mapping index, the table below displays the actual rate limits that will be used by each rate limit port group for that class of service.
  7. Click **Save** on the toolbar.
- 

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)

For information on related windows:

- [Create Rate Limit Window](#)
- [General Tab \(Rate Limit\)](#)

## ToS/DSCP Value Definition Chart

Use this chart to compare ToS and DSCP values.

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

ToS/DSCP Value Definition Chart

ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
192	0xC0	11000000	110	6	InterNetwork Control	0	0	0	110000	0x30	48	cs6
224	0xE0	11100000	111	7	Network Control	0	0	0	111000	0x38	56	cs7

## Priority-Based Rate Limits

---

Priority-based rate limits are used primarily by legacy devices. They are rate limits that are associated with one or more of the eight 802.1p priorities (0-7). When the associated priority is selected for a class of service, the rate limit becomes part of that class of service.

These rate limits are written directly to each port (unless the port is specified in the rate limit's exclusion list), and are implemented based on the 802.1p priority assigned to a data packet appearing on that port. While priority-based rate limits are not tied directly to roles or rules, they are displayed with the associated priority when you select a class of service while creating a rule, automated service, or role.

When priority-based rate limiting is implemented, the combined rate of all traffic on the port that matches the priorities associated with the rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

Once a rate limit is associated with a priority, that priority will include rate limiting wherever and however it is used, until the rate limit is deleted from Policy Manager. Also, once a priority-based rate limit is applied to a port, it will remain on the port even if the role that originally used the rate limit is no longer associated with the port. For example, if an untagged packet arrives on a port where there is no role or default priority, but the port's 802.1p priority includes a rate limit, that traffic will be rate limited. As another example, if the priority of a tagged packet matches a priority-based rate limit on a port, the traffic will be rate limited.

To configure a priority-based rate limit, you need to specify the following components:

- *Rate Limit* - The highest transmission rate at which traffic can enter or exit a port.
- *Direction* - The direction to which the limit applies (inbound or outbound traffic). In order to control traffic inbound and outbound on the same port, two rate limits must be configured (one inbound and one outbound). Inbound rate limiting takes place after a frame has been classified into one of the eight priorities. Outbound rate limiting takes place just before a frame is queued for transmission. A single frame may pass through

inbound and outbound rate limits depending on the path it takes through the device and the rate limiting configuration on the device.

- *Priority* - The 802.1p priority or priorities the rate limit is associated with.
- *Precedence* - The order in which the rate limit will be written to devices that support it. Policy Manager allows you to define as many rate limits as you wish; however, the number written to a device is restricted by the number of rate limits supported by the device. Each port on the device may utilize any or all of the defined rate limits up to the number of rate limits it supports.
- *Exclusion* - The devices/ports you wish to be excluded from the rate limit. For example, rate limiting is most often used for edge devices; therefore, you might want to exclude a device group or port group containing non-edge devices or ports.

## How to Define Priority-Based Rate Limits

---

Priority-based rate limits are supported in Policy Manager for use with legacy devices such as the E7 and E1 devices. For information on defining role-based rate limits for N-Series, S-Series and K-Series devices, see [How to Define Rate Limits](#).

Priority-based rate limits are associated with one or more of the eight 802.1p priorities (0-7). When the associated priority is selected for a class of service, the rate limit becomes part of that class of service.

When priority-based rate limiting is implemented, the combined rate of all traffic on the port that matches the priorities associated with the rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

In order to control traffic inbound and outbound on the same port, two rate limits must be configured (one inbound and one outbound).

Instructions on:

- [Defining Priority-Based Rate Limits](#)
- [Removing a Priority-Based Rate Limit](#)

### *Defining Priority-Based Rate Limits*

To define a priority-based rate limit:

1. Open the Class of Service Configuration window (available from the Policy Manager Edit menu).
2. Select the **Show all CoS Components in Tree (Advanced Mode)** option from the **Domain Managed CoS Components** menu to display the CoS tree in the left panel.
3. In the left-panel tree, expand the CoS Components folder.
4. Right-click the Rate Limits folder and select **Create Rate Limit**.
5. In the [Create Rate Limit window](#), specify the desired rate limit and click **OK**. The rate limit will be created under the left-panel Rate Limits folder. Note that rate limit actions are not supported by priority-based rate limits and are ignored.
6. Select the rate limit and display the [General tab](#) in the right panel.

7. In the Description field, click the **Edit** button and enter a description for the rate limit.
8. In the Priority-Based Configuration sub-tab:
  - a. Select Inbound or Outbound direction, depending on whether the rate limit is for inbound or outbound traffic.
  - b. Select the 802.1p priority or priorities with which the rate limit will be associated. Each 802.1p priority can have only one inbound and one outbound rate limit; therefore, if a priority is already being utilized for the selected direction, it is grayed out.
  - c. If you are creating a rate limit to be used on C2/B2 10/100 ports, select either Low to associate the rate limit with priorities 0-3 or High to associate the rate limit with priorities 4-7. You can select both Low and High if you want to associate the rate limit with priorities 0-7. If the Low or High priority is already being utilized for another rate limit, it will be grayed out. Because C2/B2 10/100 ports only support inbound rate limits, this section will be grayed out if you have selected Outbound for your rate limit Direction.
  - d. Click the Precedence **Edit** button. This opens the [Precedence tab](#), where you can change the order in which priority-based rate limits will be written to devices that support them. This is useful on legacy devices which support a varying number of rate limits.
  - e. If you want to specify any network elements to which this rate limit will *not* apply, go to the Exclusion area, click **Edit**, and make your selection from the list of network elements. Click **OK**.
9. Verify that priority-based rate limiting is enabled in the Class of Service Mode section on the device [General tab](#) or via the [Device Configuration Wizard](#).
10. Enforce.

Priority-based rate limits add to the amount of time it takes to enforce and verify roles. Once you've created your rate limits and enforced them, you may want to disable rate limits so that it takes less time to enforce. You can disable rate limits in the Class of Service Mode section of the device [General tab](#).

Once a rate limit is associated with a priority, that priority will include rate limiting wherever and however it is used, until the rate limit is deleted from Policy Manager. Also, once a priority-based rate limit is applied to a port, it will remain on the port even if the role that originally used the rate limit is no longer associated with the port.



## *Removing a Priority-Based Rate Limit*

Once a priority-based rate limit is associated with a priority, that priority will include rate limiting wherever and however it is used, until the rate limit is deleted from Policy Manager. In addition, once the rate limit is applied to a port, it remains on the port even if the role that originally used the rate limit is no longer associated with the port.

To remove a priority-based rate limit, you must delete it from Policy Manager and then perform an Enforce with priority-based rate limiting enabled. This will remove the rate limit from any ports it was applied to.

1. Open the Class of Service Configuration window (available from the Policy Manager Edit menu).
  2. Select the **Show all CoS Components in Tree (Advanced Mode)** option from the **Domain Managed CoS Components** menu to display the CoS tree in the left panel.
  3. Expand the CoS Components folder and the Rate Limits folder.
  4. Right-click the rate limit you want to remove, and select **Delete** from the menu.
  5. Verify that priority-based rate limiting is enabled in the Class of Service Mode section on the device [General tab](#) or via the [Device Configuration Wizard](#).
  6. Enforce.
- 

## **Related Information**

For information on related concepts:

- [Policy-Based Rate Limits](#)

For information on related tasks:

- [How to Create a Class of Service](#)

For information on related windows:

- [Create Rate Limit Window](#)
- [General Tab \(Rate Limit\)](#)

# How To Use Policy Manager

---

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

## How to Add and Delete Devices

---

The NetSight database contains all the devices in your network and displays them in the left-panel device tree. Console and Policy Manager share a common view of the device tree, except that only devices that support policy are displayed in the Policy Manager tree. Any changes you make to the devices are reflected in both trees.

Initially, perform a Console Discover to populate the database, or you can also use Console to import devices from a .ngf file. Once devices are added to the NetSight database, assign the devices to a [Policy Domain](#) using Policy Manager. Once you assign the devices to a domain, they are automatically displayed in the Policy Manager device tree. Only devices assigned to the domain you are currently viewing are displayed. For more information, see [How to Create and Use Domains](#).

After you have initially added your devices, you can use Policy Manager's Add Device window to add a single device to the database and the current domain.

Instructions on:

- [Using Console to Discover Devices](#)
- [Using Console to Import Devices](#)
- [Adding a Single Device](#)
- [Deleting Devices from the Database](#)
- [Disabling Policy Support from an XOS Device](#)

## Using Console to Discover Devices

Console Discover lets you to discover your network devices 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 all or a subset of the discovered devices to the NetSight database.

For step-by-step instructions, see the **How to Discover Devices** help topic in your Console online help system.

After devices are added to the database via Console Discover, they must be assigned to a Policy Domain (using Policy Manager) before they are displayed in the Policy Manager tree. Once they have been [assigned to a domain](#), the devices are automatically displayed in the appropriate groups in the Policy Manager Network Elements device tree.

## Using Console to Import Devices

The Console Import Devices feature imports device information and profiles for unique devices (ones that do not exist locally) from a .ngf file, and adds them to the NetSight database. For step-by-step instructions, see the **Importing a Device List from a File** section of the **How to Export and Import a Device List** help topic in your Console online help system.

After the devices are imported to the database, they must be assigned to a Policy Domain (using Policy Manager) before they are displayed in the Policy Manager tree. Once they have been [assigned to a domain](#), the devices are automatically displayed in the appropriate groups in the Policy Manager Network Elements device tree.

## Adding a Single Device

You can add a single device to the NetSight database using Policy Manager's [Add Device window](#). When you add a device, it is assigned to the current domain and automatically listed in the left-panel device tree. You must specify the device's SNMP profile. This information is used by Policy Manager to access and manage the device.

1. Select the Network Elements tab.
2. Select All Devices folder, right-click and select Add Device from the menu. The [Add Device window](#) opens.
3. Enter the IP address of the device you want to add.
4. Use the drop-down menu to select one of the SNMP profiles defined for device access. The **Edit** button lets you create a profile if one does not already exist.
5. Select the checkbox and enter an [SNMP context](#), if desired.
6. Select whether to use the default [nickname](#) or click **Specify** to assign a unique nickname to this device.

7. To add the device and leave the window open, click **Apply**. To add the device and close the window, click **OK**.

## Deleting Devices from the Database

When a device is deleted from the NetSight database, it is removed from all groups where it is a member in both the Policy Manager and Console device tree (and any other NetSight plugin applications).

---

**NOTE:** If you want to remove a device from a domain without deleting it from the database, you must use the [Assign Devices to Domain window](#). For more information, see [Removing Devices from a Domain](#).

---

To delete devices from the NetSight database:

1. In the left-panel Network Elements tab, select the device being deleted.
2. Right-click the device and select **Delete** from the menu. A confirmation message appears, warning that you are deleting the device from the NetSight database.
3. Click **Yes** to delete the device.

## Disabling Policy Support from an XOS Device

You can disable all policy features from an XOS device to free device resources.

---

**NOTE:** This functionality is only available on XOS devices.

---

To disable policy features from an XOS device:

1. In the left-panel Network Elements tab, select the device on which to disable policy functionality.
  2. Right-click the device and select **Disable Policy Support** from the menu. A confirmation message appears, warning that you are disabling policy support on the device.
  3. Click **OK** to disable policy support on the device.
- 

## Related Information

For information on related tasks:

- [How to Create and Use Domains](#)

For information on related windows:

- [Add Device Window](#)

## How to Add and Remove Device Groups

---

You can organize your network devices into device groups and subgroups under the My Network folder in the Network Elements tab. Organizing your devices into groups lets you perform certain operations on an entire group at once, instead of performing the operation on individual devices. A set of system-created device groups are automatically provided. When a device is created, discovered, or imported, it automatically becomes a member of the appropriate system-created group:

- All Devices - contains all the devices in the NetSight database.
- Grouped By - contains five subgroups:
  - Chassis -- contains subgroups for specific chassis in your network.
  - Contact -- contains subgroups based on the system contact.
  - Device Types -- contains subgroups for the specific product families and device types in your network.
  - IP -- contains subgroups based on the IP subnets in your network.
  - Location -- contains subgroups based on the system location.

Additionally, you can add your own device groups and subgroups under the My Network folder, however you cannot add groups under the system-created groups. A device group cannot have the same name as another device group at the same level. You cannot rename or delete a system-created group. A device can be a member of more than one group.

---

**TIP:** System-created groups are displayed with blue folders in the left-panel tree. Any group you add will display a yellow folder.

---

Instructions on:

- [Adding a Device Group](#)
- [Adding Devices to a Device Group](#)
- [Removing Devices from a Device Group](#)
- [Renaming a Device Group](#)
- [Deleting a Device Group](#)

## Adding a Device Group

1. Click the left-panel Network Elements tab.
2. Right-click on the My Network folder or any user-created group, and select **Add Device Group** from the menu. This opens the Add Device Group window.
3. Enter the device group name and click **OK**. (Device groups cannot have the same name as another device group at the same level.) You can now [add devices](#) to the device group.

## Adding Devices to a Device Group

You can add a device to a group by using the Add Device window, the Device Group Selection window, or by using drag and drop.

### *Using the Add Device Window*

Use the Add Device window to add a single device to the NetSight database and to the group selected in the tree.

1. Right-click the group to which you want to add a device and select **Add Device** from the menu. The [Add Device window](#) opens.
2. Enter 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. Select the checkbox and enter an [SNMP context](#), if desired.
5. Select whether to use the default [nickname](#) or click **Specify** to assign a unique nickname to this device.
6. Click **OK**. The new device appears in the group and is automatically added to the All Devices group.

### *Using the Device Group Selection Window*

Use the Device Group Selection window to add one or more devices from a right-panel Details View to the My Network group or a user-created group in the left-panel tree.



1. In a right-panel Details View tab, right-click the device(s) that you want to add to a group and select **Add Device(s) to Group** from the menu. The [Device Group Selection window](#) opens.
2. Select the My Network group or the desired user-created group.
3. Click **OK**. The selected device(s) appear in the group.

---

**TIP:** You can also add one or more devices from a right-panel Details View to the My Network group or a user-created group by using the copy and paste toolbar buttons or right-click menu options.

---

### *Dragging and Dropping Devices*

In the left-panel tree, you can add a device to a group by dragging a device 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. You can only drag devices to the My Network group or a user-created group.

---

**TIP:** You can also use the copy and add toolbar buttons or right-click menu options to add a device to a group in the left-panel tree.

---

#### To add a device using drag and drop:

1. In the left panel, expand the hierarchy to show the target group and the device that you want to add.
2. Select the device to be dragged and dropped.
3. Click and hold on the selected device and drag it into the target group.

#### To add a group using drag and drop:

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.

## Removing Devices from a Device Group

This function simply removes a device or devices from a device group. It should not be confused with *deleting* a device (right-clicking the device and selecting

**Delete** from the menu), which removes the device from the device group, the All Devices folder, and from the NetSight database.

1. In the left-panel Network Elements tab, expand the device group from which you wish to remove a device.
2. Right-click a single device and select **Remove from Device Group** from the menu.

## Renaming a Device Group

This function allows you to rename a device group. You cannot rename the [system-created device groups](#).

1. In the left-panel Network Elements tab, right-click the device group you wish to rename, and select **Rename Device Group**.
2. Type the device group name in the highlighted box and press **Enter**. (A device group cannot have the same name as another device group at the same level.)

## Deleting a Device Group

This function removes a device group and its devices. Only the group is deleted; the devices remain in the All Devices folder and the NetSight database. You cannot delete the [system-created device groups](#).

1. In the left-panel Network Elements tab, right-click the device group you wish to delete, and select **Delete Device Group** from the menu.
  2. A confirmation message appears. Click **Yes**.
- 

### Related Information

For information on related tasks:

- [How to Add and Delete Devices](#)

# How to Configure Anti-Spoofing

---

This Help topic describes the Policy Manager anti-spoofing feature and how to configure it. It includes the following sections:

- [Anti-Spoofing Overview](#)
- [DHCP Snooping](#)
  - [DHCP Snooping Port Types](#)
  - [DHCP MAC Verify](#)
- [Dynamic ARP Inspection \(DAI\)](#)
- [IP Source Guard](#)
- [Duplicate IP Checking](#)
- [Populating the MAC-to-IP Binding Table](#)
  - [Bindings Created by DHCP Snooping](#)
  - [Bindings Created by DAI or IP Source Guard](#)
  - [Expiration of Bindings](#)
- [Implementing Anti-Spoofing in Your Network](#)
  - [Using DHCP Snooping Only](#)
  - [Using DAI, IP Source Guard, and Duplicate IP Detection](#)
- [Anti-Spoofing Configuration](#)
  - [Port Classes](#)
  - [Managing the Binding Table](#)
- [Anti-Spoofing Configuration Steps](#)
  - [Configure Port Classes](#)
  - [Configure Ports](#)
  - [Configure Devices](#)
- [Configuration Example](#)

## Anti-Spoofing Overview

Attacks on IP networks can be performed easily using tools available on the internet today. Malicious users can spoof DHCP server response packets,

allowing them to give false information to a user for such fields as the default gateway or domain name resolution servers. Man-in-the-middle attacks can take advantage of ARP, allowing hackers to redirect user traffic through their own devices to and from the default gateway. A hacker can then spy on the private information being sent from the user, without either the user or gateway knowing. A malicious user can spoof an innocent user's IP address, allowing the malicious user to bypass other possible security features of a network that are based on a user's subnet.

The Policy Manager anti-spoofing solution provides a flexible and secure approach to IP spoofing detection and prevention. To mitigate the effects of these types of attacks on a network, a source MAC address to source IP address binding table is created. Then, based on the entries in the binding table, action can be taken against violating users.

There are three basic tools used to detect source MAC address to source IP address associations and populate the binding table:

- DHCP snooping
- Dynamic ARP inspection (DAI)
- IP source guard

All three methods can create MAC-to-IP bindings in the binding table, although both DAI and IP source guard can be configured to run in inspection only mode, which would not create bindings. Bindings created as a result of DHCP exchanges on trusted ports using DHCP snooping take precedence over bindings created through dynamic ARP inspection or IP source guard.

Use of all three tools allows bindings to be created for users in a network where DHCP is not in use or where a DHCP exchange has not occurred since the anti-spoofing feature has been enabled.

The actions that may be taken against a violating user include:

- Logging a syslog message
- Generating an audit trap
- Putting the user in quarantine, as defined by a quarantine role.

## DHCP Snooping

DHCP snooping provides the foundation for IP spoofing detection and prevention. DHCP ACK packets received from a DHCP server on a "trusted" port

create a MAC-to-IP address binding for the user along with the lease time and expiration. DHCP ACK packets received on "untrusted" ports are dropped.

On untrusted ports on edge devices, DHCP MAC Verify can be configured to verify that the source MAC address and the client hardware address match in DHCP client packets that transit the ports. If the addresses match, the packets are forwarded. If the addresses do not match, the packets are dropped.

### *DHCP Snooping Port Types*

In a DHCP snooping, ports are set to one of three port types that determine anti-spoofing behavior. Anti-spoofing is typically configured on the edge of the network, with ports assigned one of the following port types:

- **Trusted** – When port type is set to trusted, DHCP server traffic is accepted and used to create bindings in the MAC-to-IP address binding table. Typically, only a port that is connected to a DHCP server would be set to trusted.
- **Bypass** – When port type is set to bypass, snooping of DHCP server traffic does not take place on the port. Typically, uplink ports out to the network would be set to bypass, as traffic would not be originating from that port.
- **Untrusted** – When port type is set to untrusted, the untrusted server counter is incremented when DHCP server traffic (DHCP ACK) is detected on the port, and the packets are dropped. DHCP RELEASE and DECLINE messages, sent by a client to free its IP address for use by another, are dropped if they are for a MAC address in the binding table that is on another port. If DHCP MAC Verify is enabled and the source MAC address does not match the Client Host Address in the DHCP payload (CHADDR), the packets are dropped. Typically, all edge ports with users would be set to untrusted.

### *DHCP MAC Verify*

All UDP traffic contains MAC address information in the packet header. DHCP traffic contains additional MAC address information in the payload. When DHCP MAC verification is enabled, DHCP snooping verifies that the source MAC address in the UDP packet frame header matches the MAC address specified in the DHCP payload as the Client Host Address (CHADDR). If the addresses do not match, the packet is dropped.

DHCP MAC verification is a network edge feature that should be enabled on ports transited by DHCP client packets. For DHCP MAC verification to be operational:

- DHCP snooping must be enabled on the device and on the port.
- The port type must be set to untrusted.

## Dynamic ARP Inspection (DAI)

Dynamic ARP inspection uses the MAC-to-IP address binding table to ensure that ARP packets have the proper MAC-to-IP binding. Limiting ARPs to the bound addresses in the table prevents malicious users from inserting themselves in between the end user and a gateway and poisoning network device ARP caches, or succeeding in man-in-the-middle attacks.

When an ARP packet enters the switch, the source MAC and IP addresses are compared to the entry in the table. If the packet data conflicts with the binding in the table, the IP change is counted and logged for the binding and any configured actions are taken against the user. If the packet data does not conflict with the binding table it will be forwarded. If the packet data does not exist in the binding table, it will be added unless DAI is enabled in inspection only mode.

## IP Source Guard

IP source guard is another means to restrict IP traffic and take action against violating users. It is particularly beneficial in an environment not limited to edge devices or one in which DHCP is not the sole proprietor of network IP addresses.

IP traffic on a port is inspected to ensure that a user's MAC and IP addresses are found in the binding table created by DHCP snooping. Changes to a user's IP address are counted and action is taken, as configured. Like DAI, IP source guard will add entries to the MAC-to-IP binding table unless it is enabled in inspection only mode.

## Duplicate IP Checking

In addition to the anti-spoofing tools described above, the anti-spoofing feature can also be configured to log duplicate IP addresses when they are bound to different MAC addresses, using syslog messages and audit traps. This situation is usually due to a misconfiguration in the network and is generally not indicative

of an attack, but can be a worthwhile event to record, as administrative action may be needed to reconcile the condition. These duplicate IP addresses are only detected upon a user's binding change, and do not apply to duplicate IP addresses over ports for the same MAC address (for example, if a single user moves from one port to another).

## Populating the MAC-to-IP Binding Table

The anti-spoofing MAC-to-IP binding table can be populated through DHCP snooping, dynamic ARP inspection, and IP source guard. Regardless of which of these three methods are used, an entry cannot be added if there is not already an entry for the user's MAC address in the multi-auth session table (displayed in the End User Sessions table in the device [Port Usage tab](#).)

### *Bindings Created by DHCP Snooping*

DHCP snooping watches DHCP exchanges to create a MAC-to-IP address binding for a client. A basic DHCP client/server exchange is as follows:

1. client > server: DISCOVER
2. server > client: OFFER
3. client > server: REQUEST
4. server > client: ACKNOWLEDGE

It is the acknowledgment from the server that creates the binding, and the server message is considered authoritative. (No other security measures, other than those described here, are used to ensure that the server is legitimately responding to a client request.)

The ACK message includes the client hardware address and the client's confirmed IP address. It is the client hardware address (not the MAC destination address) that is used in determining if there is already an entry in the multi-auth session table for the user, to which the IP address will be bound. If there is no entry in the session table for the client, a syslog message will be generated.

Only DHCP server ACK messages received on trusted ports will populate MAC-TO-IP address bindings. On untrusted ports, any DHCP server packets are recorded (that is, the counter is incremented), but they are not used to populate the MAC-to-IP address bindings. If policy is properly configured, the packets will be dropped or the port will be shut down, as specified by the role assigned to the port. Bypass ports ignore all DHCP server packets for purposes of populating the binding database.

DHCP server messages are limited to trusted ports, so the bindings that are created by them are not intended to be recorded as violations. In the case that a server sends a client a new binding with a different IP address before the current binding's lease has expired, the event will trigger a syslog message, but will not increment the violation counter.

### *Bindings Created by DAI or IP Source Guard*

When DAI or IP source guard are enabled, the other traffic being inspected (ARP or IP) can also populate the IP address bindings table. With ARP inspection, the sender MAC and IP and the target MAC and IP from the ARP payload are used to populate the bindings, as provided by the ARP request or reply. With IP inspection, the source MAC address and IP address are used in creating these bindings.

If a binding already exists for a user due to DHCP, and the lease time has not expired, the DHCP binding takes precedence and a violation is recorded, but the binding does not change. If there is an entry for the user in the multi-auth session table and DHCP snooping has not provided a MAC-to-IP address binding table entry, the ARP or IP traffic can create the MAC-to-IP address binding table entry. This form of binding creation allows for the anti-spoofing feature to be used in environments that are not on the edge or are not able to monitor and process all DHCP exchanges on the network for attached users.

### *Expiration of Bindings*

IP address bindings will timeout when a lease expires, a DHCP release frame is received, or upon manual clearing of an entry, whichever occurs first. For DHCP-snooping created bindings, after the lease expires, the binding also expires. However, for DAI and IP inspection, the counter resets after the timeout period, but the binding remains active (restarts the timer).

When you manually set a timeout period, be aware that the lease time defined in the DHCP server scope takes precedence over manually set timeouts.

## **Implementing Anti-Spoofing in Your Network**

### *Using DHCP Snooping Only*

In a network edge environment where DHCP is the exclusive provider of IP addresses, DHCP snooping can be used by itself to record all end user DHCP interactions, creating a MAC-to-IP address binding for each connected user.



Optionally, MAC Verify can be configured on untrusted ports to verify that the client hardware address in the DHCP packet matches the source MAC address of the packet. If it does not, it is dropped. This is a more robust security feature that can be used on the edge of the network where it is expected that the client requests are coming from the client, not a different switch, router, or AP.

In this scenario, DHCP snooping ensures that server packets are only handled where appropriate, that malicious users do not release or decline DHCP IP address assignments for other users, that DHCP client request packets are coming from the actual client (MAC Verify), and that the MAC-to-IP address binding database is populated. No actions are taken against users whose IP address assignment changes due to DHCP (where the server responses are on a trusted port), and user counters don't increment.

In an environment away from the network edge, if DAI and IP source guard are disabled or configured for inspection only, DHCP exchange packets could be missed. For example, link loss at the distribution or core layer would not necessarily cause DHCP renewals from the end users at the edge, thus the binding table would not be repopulated and users could suffer the consequence of unintended violation actions (for example, denial of service).

However, there are still benefits obtained from using DHCP snooping by itself away from the network edge. It allows for user accounting (user IP address change counters) and for the population of the MAC-to-IP address binding table from known DHCP servers. The binding table will then allow user leases to run for the configured lease time used on the network.

In this scenario, an administrator should recognize that configuring any actions that limit a user's traffic after a violation could potentially disrupt network traffic for an otherwise legitimate user. Generally, this configuration would not be used away from the network edge to quarantine or otherwise limit the user's traffic, as these limitations could be manipulated to cause denial of service attacks against a user.

### *Using DAI, IP Source Guard, and Duplicate IP Detection*

Once DAI is enabled or set to inspection only, ARP packet inspection occurs. On those ports, all ARP traffic is intercepted and the MAC and IP address of the ARP is verified against the entry in the MAC-to-IP address binding table. Actions may be taken against the user if there is a violation.

Similarly, if IP source guard is enabled or configured for inspection only, IP traffic is intercepted and verified against the binding table. Once a connection is

created, that traffic won't be inspected again unless the source IP address associated with the MAC address changes. As IP address changes are detected, the anti-spoofing feature will take action if there is a violation.

If the duplicate IP detection feature is enabled, when new MAC-to-IP bindings are created or current bindings are changed, an IP address lookup is performed on the binding table to verify that the IP is not currently in use. If it is in use, a syslog message and trap are sent.

## Anti-Spoofing Configuration

You can enable and disable anti-spoofing on a per-device basis. When the feature is disabled on the device, no anti-spoofing features are active. Anti-spoofing must be enabled on the device before port values are considered when inspecting traffic. The default value for all anti-spoofing features on the device and port, is disabled.

DHCP snooping and MAC Verify are enabled or disabled per port. DAI and IP source guard are enabled, disabled, or set to inspection only per port. Duplicate IP Checking is enabled or disabled per device.

Each port must have its port type set to trusted, untrusted, or bypass. Port type determines how DHCP snooping will handle the port's traffic. DHCP server messages are only processed on trusted ports. On untrusted ports, DHCP server messages are counted in the untrusted packet counter (per port) and dropped. On bypass ports, DHCP server messages are ignored (that is, they do not affect the MAC-to-IP binding database), but they are not dropped. Ports are untrusted by default.

### *Port Classes*

Enabling anti-spoofing on both the device and port level results in snooping frames, but it does not necessarily result in any actions taken on IP address binding violations. For this, you must define threshold values and resulting actions that will be used when MAC-to-IP address binding violations occur.

To do this, port classes must be defined and ports added to the appropriate port class. Up to three port classes can be configured on the switch. For example, you might configure a port class for your edge ports and another port class for your uplink ports. You might also want to configure a port class for ports with statically assigned addresses, allowing for a stricter threshold configuration. Another option is to configure port classes for ports that are using different

methods to create MAC-to-IP bindings, such as DHCP snooping ports in one class and IP source guard ports in another class.

Port classes are configured with thresholds and actions. Up to six thresholds can be configured per port class, and each threshold can be assigned one or more of the following actions: sending syslog messages, sending an audit trap, or applying a quarantine policy. If the quarantine action is specified, you must associate a valid quarantine policy with the quarantine action.

If you have only one anti-spoofing detection type enabled on the port (for example, DHCP snooping), the class thresholds and actions are configured for that anti-spoofing detection type. If multiple anti-spoofing types are enabled on a port, (for example, DHCP snooping and dynamic ARP inspection), the class thresholds and actions must take into account any combination of anti-spoofing events for both configured anti-spoofing types.

### *Managing the Binding Table*

You can delete an entry in the MAC-to-IP binding table for a device using the device Anti-Spoofing tab in Policy Manager. Clearing the binding also clears the IP address change count associated with the user. Alternatively, you can clear the IP Change Count without clearing the current binding.

You can also view a binding table for a specific port from the Anti-Spoofing tab in the Port Properties window. The same options for clearing the IP Change Count and deleting bindings are available.

## **Anti-Spoofing Configuration Steps**

Use the following steps as a guide for configuring anti-spoofing on your network. Typically, anti-spoofing is configured on the edge devices on your network. You will need to configure anti-spoofing at both the device and port level.

### *Configure Port Classes*

For each device where anti-spoofing will be enabled, configure the [port classes](#) that define the threshold values and resulting actions that will be used when MAC-to-IP address binding violations occur. Up to three port classes can be configured per device.

1. Select a device in the left-panel Network Elements tab and then select the right-panel [Anti-Spoofing tab](#).
2. Select the Device Configuration sub-tab.
3. In the Violation Actions section, configure the port classes for the device. Click on a Port Class tab and enter a name for the port class.
4. Set the Binding Lease Time, which is the number of seconds a binding will exist before being removed by the device.
5. Configure the thresholds and actions for the class. Select an action index number in the table and click the **Edit Action(s)** button or double-click the row. The Edit Actions window opens where you can configure the threshold value and action. If you assign a quarantine action, you must associate a valid quarantine policy with the quarantine action. For more information, refer to [How to Create a Quarantine Role](#).
6. Assign the appropriate ports to each port class you configure. Use the **Add/Remove Ports** button to add or remove ports to or from the class.
7. Click **Apply** to save your changes.

### *Configure Ports*

Configure anti-spoofing for the ports on each device where anti-spoofing will be enabled.

1. In the device Anti-Spoofing tab, select the Port Configuration sub-tab.
2. In the table, select the ports that you will set as Trusted. Right-click and use the menu to:
  - a. Set the Port Type to Trusted.
  - b. Set DHCP Snooping to Enabled.
  - c. Set DHCP MAC Verify to Disabled.
3. Select the ports that you will set as Untrusted. Right-click and use the menu to:
  - a. Set the Port Type to Untrusted.
  - b. Set DHCP Snooping to Enabled.
  - c. Optionally, set DHCP MAC Verify to Enabled.
4. Select the ports that you will set as Bypass. Right-click and use the menu to:

- a. Set the Port Type to Bypass
  - b. Set DHCP Snooping to Disabled.
  - c. Set DHCP MAC Verify to Disabled.
5. Optionally, enable dynamic ARP inspection on the desired port or ports. Select the ports in the table, right-click and use the menu to set dynamic ARP inspection to Enabled, Disabled, or Inspection Only.
  6. Optionally, enable IP source guard on the desired port or ports. Select the ports in the table, right-click and use the menu to set IP source guard to Enabled, Disabled, or Inspection Only.

You can also set anti-spoofing parameters for a single port using the [Port Properties Anti-Spoofing tab](#).

### *Configure Devices*

For each device, enable anti-spoofing and set anti-spoofing parameters.

1. In the Anti-Spoofing tab, select the Device Configuration sub-tab.
2. Use the drop-down menu to set Anti-Spoofing to Enabled on the device.
3. Use the drop-down menu to set Audit Traps to Enabled on the device, if desired. This must be enabled if you have configured an audit trap as a threshold action, in order for the trap to be sent.
4. Change the [Audit Trap Interval](#) if desired. The default is 60 seconds.
5. Enable [Duplicate IP Checking](#), if desired.
6. Click **Apply** to save your settings.

## Configuration Example

The following example configures anti-spoofing features on a switch at the edge of the network, where two ports are connected to a DHCP server and the rest of the ports are connected to users. DHCP snooping is configured on the ports connected to the DHCP server so the binding table will be populated by DHCP snooping.

User ports 10 through 40 are configured for dynamic ARP inspection and IP source guard inspection, but are enabled for inspection only, since the binding table entries are added by DHCP snooping on the DHCP server trusted ports. Also, DHCP snooping MAC Verify is enabled on the untrusted user ports.

As part of the configuration:

- Two port classes are configured: one for Server ports and one for User ports. Binding lease time, threshold, and action values for each port class are configured.
  - The two ports connected to the DHCP server are configured as trusted ports and have DHCP snooping enabled.
  - All user ports are configured as untrusted ports and have DHCP snooping enabled. DHCP MAC Verify is also enabled on all user ports.
  - Dynamic ARP inspection and IP source guard are configured for inspection only on user ports 10 through 40.
  - Both server ports are assigned to the Server port class.
  - All user ports are assigned to the User port class.
  - Anti-spoofing is enabled on the device.
  - Audit Traps are enabled on the device and the audit trap interval is changed to 30 seconds.
  - Duplicate IP checking is enabled on the device.
- 

### Related Information

For information on related tasks:

- [Device Anti-Spoofing Tab](#)
- [Port Properties - Anti-Spoofing Tab](#)

## How to Configure CEP

---

The CEP (Convergence End Point) feature provides support for CEP products such as IP phones. Using this feature, you can select the CEP product types supported on a device, and map a role for each type. Then, when a convergence endpoint (such as an IP phone) connects to the network, the device identifies the type of endpoint and applies the assigned role. In addition to configuring CEP on a device, you must also enable CEP protocols on each port. Once you have configured CEP on the device and each port, you can monitor CEP product activity using the Port Usage tabs.

Use the [Device Configuration Wizard](#) and [Port Configuration Wizard](#) to configure CEP on multiple devices/ports, or follow these steps to enable it on a single device and port.

1. Select a device in the left-panel Network Elements tab, and click the [Authentication tab](#) in the right panel.
2. In the Authentication Type section, select the appropriate CEP checkbox: Single User or Multi-User. If the device does not support the CEP feature, the CEP checkboxes are grayed out.
3. For Authentication Status, select Enabled.
4. If you have configured Multi-User authentication types, set the authentication type precedence. This allows you to set the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.
5. Click **Apply** to set any changes you have made in this section.
6. At the bottom of the window, click on the CEP tab.
7. The [CEP Detection sub-tab](#) lists the CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected. Click **Add** to open the Add CEP Detection Rule window where you can create your detection rules. (For information on creating rules, see the [Add CEP Detection Rule window](#) help topic.) Your rules will be added to the list. To remove a rule from the list, select the rule and click **Remove**. To edit a rule, select the rule

and click **Edit**. The Edit CEP Detection Rule window opens where you can edit the rule's parameters.

8. Click **Apply** to set any changes you have made in the CEP Detection sub-tab.
  9. The [CEP Role Mappings sub-tab](#) lists the CEP types supported by the device and the role mapped to each type. Click **Add** to open the Add CEP Mapping window where you can select a CEP product type and map a role for that type. Your selections will be added to the list. To remove a CEP type from the list, select the type and click **Remove**. To edit a CEP type in the list, select the type and click **Edit**. The Edit CEP Mapping window opens where you can select a different CEP type and/or role.
  10. Click **Apply** to set any changes you have made in the CEP Role Mappings sub-tab.
  11. Now, select the right-panel Details View tab and expand a slot or ports grouping.
  12. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the Authentication Configuration tab (in the top row of tabs).
  13. Select the [CEP Access sub-tab](#). The CEP Access table lists the protocols supported by this device.
  14. Use the checkboxes to enable or disable CEP protocols for this port.
  15. Click **Apply** to set any changes you have made in the tab.
  16. Repeat steps 12 through 15 for each port on the device where you want to enable CEP support.
- 

## Related Information

For information on related tasks:

- [Using the Device Configuration Wizard](#)
- [Using the Port Configuration Wizard](#)

For information on related tabs:

- [Authentication Tab \(Device\)](#)
- [Port Properties - Authentication Configuration Tab](#)



- [Port Usage Tab \(Device\)](#)
- [Port Properties - Port Usage Tab](#)

## How to Configure Devices

---

In Policy Manager, you can configure devices for [authentication](#), whereby users identify themselves to the network and are given customized access capabilities based on what role they serve in the organization. Policy Manager uses a RADIUS server and an authentication-enabled switch to allow the active role on a port to be dynamically assigned, based on the user's login.

You can configure authentication for a single device or for multiple devices. You can also configure authentication parameters on individual ports (see [How to Configure Ports](#)), but you need to configure and enable authentication on the device before any port authentication settings will take effect.

You can configure devices in two ways:

- **Using the Device Configuration Wizard:** The Device Configuration Wizard is a series of windows that lets you define a configuration, then apply it to the devices of your choosing. You can use this method to configure a single device, but it is especially useful for configuring multiple devices.
- **Using the Device Tabs:** This method enables you to configure or modify the same options found in the Device Configuration Wizard, but for a selected device, using the right-panel device tabs.

Instructions on:

- [Using the Device Configuration Wizard](#)
- [Using the Device Tabs](#)

### Using the Device Configuration Wizard

The Device Configuration Wizard is a series of windows enabling you to define an authentication configuration, then apply it to the devices of your choosing. You can elect to configure authentication settings only, RADIUS client/server communication settings, or both. You can also configure MAC Locking, Rule Accounting, and CEP (Convergence End Point) Role Mapping for the devices, and a device-level role for Matrix C1 devices only.

The Wizard also lets you create a *device configuration template* based on a device configuration so that you can easily configure devices that have the same authentication requirements. Once you create the template you can reuse it

whenever you need that specific device configuration by simply loading the template into the Device Configuration Wizard.

1. From the menu bar, select **Tools > Device Configuration Wizard**.
2. This step depends on whether or not you are using a Device Configuration Template:
  - **To use a Device Configuration Wizard Template**, click the **Load** button and select the template from the list in the Open Template window. After the template has loaded, you can select **Jump to Device Selection** to [select your devices](#), or you can proceed with the wizard and [select options to configure](#) to edit the template configuration.
  - **If you are not using a using a Device Configuration Wizard Template**, proceed with selecting options to configure.

### *Select Options to Configure*

In the **Device Configuration window**, select the components you wish to configure from the three tabs: Authentication, RADIUS, and General.

#### **Authentication Tab**

Lets you specify the authentication type(s) you want to configure. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and a single user per port (Single User Authentication). Refer to the NetSight Firmware Support tables for information on the authentication types supported by each device type. For more information about each type of authentication, see [Authentication Types](#).

---

**WARNING:** Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, will log off any currently authenticated users.

---

#### **RADIUS Tab**

Select the options related to the RADIUS server(s) and RADIUS client devices that you want to configure.

- **RADIUS Authentication Server(s)** - Lets you add or remove the RADIUS servers that will be used for authentication purposes.
- **RADIUS Accounting Server(s)** - Lets you add or remove the RADIUS servers that will be used for accounting purposes.

- **RADIUS Authentication Client Settings** - Lets you configure and enable communication between the device (RADIUS client) and a RADIUS server or servers, for the purposes of authentication.
- **RADIUS Accounting Client Settings** - Lets you configure and enable communication between the device (RADIUS client) and a RADIUS server or servers, for the purposes of accounting.
- **Application Shared Secret** - Lets you set up a password that encrypts communication between Policy Manager and the devices for retrieving and setting RADIUS information.
- **RADIUS Response Mode** - Lets you select the RADIUS response attribute that the device should use for authentication.

## General Tab

Select the general device options you want to configure.

- **MAC Locking** - Lets you enable [MAC Locking](#) on devices that support it.
- **Device Level Role (C1 Only)** - On Matrix C1 devices, you can set a device-level role that configures the services and rules for all ports on the device. Due to a limitation of the C1 devices, services and rules from the role returned from authentication cannot be applied to the port. The services and rules from this device-level role will be used instead.
- **Rule Accounting** - Lets you enable Rule Accounting on devices that support it. Rule accounting and rule hit reporting provide the ability to collect data on how policy rules are being used on your network. Once you have configured the accounting and reporting functionality, you can view the rule usage data that is collected using the Rule Usage tabs or the Policy Rule Hit Reports.
- **Class of Service Mode** - Lets you select the Class of Service mode on the devices you are configuring. Classes of service can be assigned as a classification rule action, as part of the definition of an automated service, or as a role default.
- **Invalid Role Action** - Lets you specify what happens to a user that gets an unknown or invalid role.
- **RFC3580 VLAN Authorization Status** - Lets you enable or disable RFC 3580 VLAN Authorization on devices that support it.

## Configure Settings

The sequence of windows you see next depends on the selections you made in the Device Configuration window.

**NOTE:** Each window provides the option to use the current configuration on the device(s), or set a new configuration. If you select **Use Current Configuration on Device(s)**, the default settings in the window are visible, but are unavailable for entry or editing. Keep in mind that these values do not necessarily reflect the current settings on the device.

### If you have selected to configure Authentication

All the windows you could see are listed below, but only those related to the Authentication type(s) you selected will actually appear.

#### *Authentication Configuration Window*

This window varies depending on the authentication types you have selected. Specify the authentication settings you want to configure:

#### **General Authentication Settings**

Lets you enable or disable authentication status.

#### **Global Timeout Settings**

Lets you set Session Timeout and Session Idle Timeout values.

#### **Web-Based**

Select the web-based authentication parameters you wish to configure. These parameters may not be supported on every device. Refer to the NetSight Firmware Support tables for information on what features are supported on the various device types.

- **Enhanced Login Mode** - Lets you enable the Enhanced Login Mode which causes the authentication web page to be displayed regardless of whether the URL entered into the browser by the end user is the Web Authentication URL or not.
- **Web Authentication URL** - Lets you enter the URL for your authentication web page.
- **Web Authentication IP Address** - Lets you enter the IP address of your authentication web page server.
- **Web Page Banner** - Lets you customize the banner the users see at the top of the authentication web page. For example, you might include your

company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it would not be appropriate to include "Welcome to [Your Company]" in the banner.

- **Web Authentication Logo Display Status** - Lets you specify whether to show or hide the Extreme Networks logo on the Web Page Banner.
- **Guest Networking** - Lets you enable guest networking which allows any user to access the network and obtain a guest policy without having to know a username or password.
- **Redirect Time** - For devices with Enhanced Login Mode enabled. Lets you specify the amount of time (in seconds) before the end user is redirected from the authentication web page to their requested URL.
- **DNS Server Configuration** - Lets you add your DNS domain name and server addresses to support the Enhanced Login Mode.

### MAC-Based

Select the MAC authentication parameters you wish to configure:

- **MAC User Password** - Lets you enter the password to be used for MAC authentication (1-32 characters).
- **MAC Mask** - Lets you select a mask. Masking a MAC address is only supported on certain devices.

### CEP-Based

Select the CEP authentication parameters you wish to configure:

- **CEP Role Mapping** - Lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence endpoint (such as an IP phone) connects to the network, the device identifies the type of endpoint and applies the assigned role.
- **CEP Detection** - Lets you create CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected.

### *General Authentication Settings Window*

Select whether to enable or disable the authentication type (Authentication Status) for the device(s). Leaving the status disabled gives you the ability to configure and reconfigure authentication settings without affecting your

network until authentication configuration is complete. If you have selected multiple authentication types, all of the authentication types selected will be enabled or disabled with this one setting.

---

**WARNING:** Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, will log off any currently authenticated users.

---

---

**CAUTION:** Setting the authentication status to Enabled will affect communications through the front panel ports. Any front panel being used for management should be set to inactive/default mode before setting authentication status to Enabled. If you elect to enable authentication, an Authentication Status window appears offering you choices for actions that will take effect on front panel ports after the wizard is finished. These options are described in detail in the Authentication Status window. (If you choose the **Select Ports to set to Inactive/Default Role** option, the [Set Authentication Port Mode to Inactive/Default Role window](#) will appear at the end of the wizard after you've selected the devices to which the configuration will apply and clicked **Finish**.) After making your selection, click **OK** to return to the Authentication Settings window.

---

If you selected Web-Based as an Authentication Type, enable or disable [WINS/DNS spoofing](#) for DHCP clients, and select the [Authentication Protocol](#) being used.

If you are configuring Multi-User Authentication, you can set the Authentication Type Precedence. This allows you to set the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). Select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence.

---

**WARNING:** Leaving the default precedence is recommended. In particular, changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type can cause problems.

---

### *Global Timeout Settings Window*

Specify session and idle timeout values for each of the authentication types:

**Session Timeout:** Enter the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

**Session Idle Timeout:** Enter the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that no idle timeout will be applied.

These values may be superseded by a session timeout and an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send a session timeout or an idle timeout value in its authentication response.

### *Enhanced Login Mode Window (web-based authentication only)*

Enabling this feature causes the authentication web page to be displayed regardless of whether the URL entered into the browser by the end user is the Web Authentication URL or not.

### *Web Authentication URL Window (web-based authentication only)*

Enter the URL for your authentication web page. Users access the authentication web page from a browser using this URL. The **http://** is supplied. Alphabetical characters, numerical characters and dashes are allowed as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

### *Web Authentication IP Address Window (web-based authentication only)*

Enter the IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the hosts file of each client.

### *Login Web Page Banner Window (web-based authentication only)*

Enter any information you want to convey to your users at the top of your authentication web page. For example, you might enter your company name, and information on what to do if the user has questions or problems. The **Default** button allows you to reset the banner to default text provided in a text file (pwa\_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa\_banner.txt file, located in the top level of the Policy Manager install director



### *Web Authentication Logo Display Status Window (web-based authentication only)*

Specify whether to show or hide the Extreme Networks logo on your authentication web page.

### *DNS Server Configuration Window (web-based authentication only)*

Configure your DNS domain name and server addresses to support the Enhanced Login Mode on Matrix E1 devices. Enter your local DNS Domain Name (for example, ExtremeNetworks.com), and your local DNS Server IP addresses. Enter an IP address and click **Add** to add a server address. Select an address and click **Remove** to remove an address from the list. Addresses are used in the order they are listed.

### *Guest Networking Window (web-based authentication only)*

Guest networking allows any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, allowing them to log in as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

**NOTE:** Guest networking is designed for networks using web-based authentication, with [port mode](#) set to Active/Discard.

Make the following guest networking selections:

**Guest Networking Status:** Use the drop-down list to specify guest networking status:

- **Disable** -- Guest networking will be unavailable.
- **Local Auth** -- Guest Networking will be enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified [Guest Name](#). Once the user submits the login page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.
- **RADIUS Auth** -- Guest Networking will be enabled. The user accesses the login web page, where the username field is automatically filled in with the specified [Guest Name](#), and the password field is masked out with asterisks. Once the user submits the login page using these credentials, the value of

the [Guest Password](#) will be used for authentication. Following successful authentication from the RADIUS server, the port will apply the policy returned from the RADIUS server. The port mode must be set to Active/Discard mode.

**Guest Name:** Enter the guest name. This is the username that Guest Networking will use to authenticate users, and is displayed automatically on the login web page.

**Guest Password:** If you have selected RADIUS Auth, enter the guest password that will be used for authentication.

### *Redirect Time Window (web-based authentication only)*

This setting applies to devices with Enhanced Login Mode enabled. Enter the amount of time (in seconds) before the end user is redirected from the authentication web page to their requested URL. Click the **Default** button to enter the default value of 30 seconds.

An end-system using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. Redirect Time specifies the amount of time allowed for the end station to complete this process and begin using its official IP address. The default value of 30 seconds is adequate for most networks; however, some networks may require a longer or shorter time period. If the Redirect Time is not long enough, the browser times out while attempting to load the requested URL. In networks that only use static IP addresses, a Redirect Time of 5 to 10 seconds is usually sufficient; a value of less than 5 seconds is not recommended.

For example, if a user (in Enhanced Login Mode and a Redirect Time of 30 seconds) enters the URL of "http://ExtremeNetworks.com", they will be presented the authentication web page. When the user successfully authenticates into the network, they will see a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds".

### *MAC Mask Window*

Select a MAC mask that will be used for MAC authentication. (Masking a MAC address is only supported on certain devices.) Using a mask provides a way to authenticate end stations based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturer's ID portion of the MAC address. The MAC Mask is passed to the RADIUS server

for authentication after the primary attempt to authenticate using the full MAC address fails.

#### *MAC User Password Window*

Enter the password that will be passed to the RADIUS server for MAC authentication (1-32 characters).

#### *CEP Role Mapping Window*

Use the **Add** button to select the CEP product types supported on the device, and map a role for each type.

#### *CEP Detection Window*

Use the **Add** button to create your CEP detection rules. (For information on creating rules, see the [Add CEP Detection Rule window](#) help topic.)

#### **If you have selected to configure RADIUS**

All the windows you could see are listed below, but only those related to the RADIUS options you selected will actually appear:

#### *RADIUS Authentication Server(s) Window*

Add or remove RADIUS servers to use for authentication purposes. The order in which the servers are listed is the order of priority for the servers; the device will try to communicate with the RADIUS server at the top of the list first.

*To add a RADIUS server:* Click **Add** to open the [Add RADIUS Authentication Server window](#), where you will specify the information required for communication between the devices and the RADIUS server.

*To remove a RADIUS server:* Select the server in the table and click **Remove**.

**NOTE:** Setting a new configuration for RADIUS servers will remove/replace any RADIUS servers currently configured on the device(s).

#### *RADIUS Accounting Server(s) Window*

Add or remove RADIUS servers to use for accounting purposes. The order in which the servers are listed is the order of priority for the servers; the device will try to communicate with the RADIUS server at the top of the list first.

To add a RADIUS server: Click **Add** to open the [Add RADIUS Accounting Server window](#), where you will specify the information required for communication between the devices and the RADIUS server.

To remove a RADIUS server: Select the server in the table and click **Remove**.

**NOTE:** Setting a new configuration for RADIUS servers will remove/replace any RADIUS servers currently configured on the device(s).

#### *RADIUS Authentication Client Settings Window*

Make the following RADIUS client selections:

**RADIUS Client Status:** Enable or disable the RADIUS client. If enabled, the device becomes a RADIUS client and will communicate with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS server.

**Number of Retry Attempts:** Enter the number of attempts the RADIUS client will make in contacting each RADIUS authentication server before giving up and trying the next RADIUS server on the list. Valid values are 1-65535.

**Retry Timeout Duration (seconds):** Enter the number of seconds to wait for the RADIUS authentication server to respond before trying again. Valid values are 1-65535.

#### *RADIUS Accounting Client Settings Window*

Make the following RADIUS client selections:

**Client Accounting Status:** Enable or disable RADIUS Accounting for SNMPv3 devices that support it. RADIUS Accounting is used by a device (the RADIUS client) to save accounting data on a RADIUS server. If enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server.

**Accounting Update Interval (minutes):** Enter the number of minutes between accounting updates, when collected accounting data is sent from the device (RADIUS client) to the RADIUS accounting server. Valid values are 1-65535. It is recommended that the value be greater than 10 minutes, and careful consideration should be given to its impact on network traffic.

### *Application Shared Secret Window*

Select from the following choices the [application shared secret](#) you want to be used for communication between Policy Manager and the device when setting or retrieving RADIUS information.

**Auto-Generate an application shared secret:** If you want the system to generate a secure key [automatically](#), select this button.

**Use the following application shared secret:** If you want to [create your own shared secret](#), select this button and type in a 32-character string with optional dashes or spaces, typically xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx.

**Use the default application shared secret:** If you want to use the [default application shared secret](#), click this button. This is not recommended, as it is less secure than a non-default shared secret.

---

**WARNING:** It is important to remember the Application Shared Secret, since the shared secret specified in Policy Manager must match the shared secret on the device in order to change the shared secret. If you delete and recreate the device model, you will have to supply the correct Application Shared Secret in the device's RADIUS tab in order to retrieve or input RADIUS settings in the RADIUS tab. If you're using an Auto-Generated or User-Defined Application Shared Secret and you clear NVRAM on the device, you will need to go to the RADIUS tab for the device in Policy Manager and change the Application Shared Secret back to "Default" in order to regain access to the RADIUS information in that tab. Once Policy Manager and the device are using the same (Default) Application Shared Secret, then the Application Shared Secret can be changed to be either Auto-Generated or User-Defined.

---

### *RADIUS Response Mode Window*

Select the RADIUS response attribute that the device should use for authentication:

**Filter ID:** The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it will be ignored.

**VLAN Tunnel Attribute:** The VLAN Tunnel Attribute is used and the [Authentication-Based VLAN to Role Mappings](#) are applied, if present. If a Filter ID is returned, it will be ignored.

**Filter ID With VLAN Tunnel Attribute:** Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel

Attribute replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

### If you have selected General

All the windows you could see are listed below, but only those related to the options you selected will actually appear:

#### *MAC Locking Window*

Configure [MAC Locking](#) status on the device. Setting MAC Locking to Enabled will allow the device to lock MAC addresses to all ports that have the MAC Locking feature enabled.

#### *Device Level Role (C1 Only) Window*

Use the drop-down list to select a device-level role that configures the services and rules for all ports on the device. Select the Clear the current default role option to set the device-level role back to <None>.

#### *Rule Accounting Window*

Configure [rule accounting](#) on the device. Rule accounting and rule hit reporting provide the ability to collect data on how policy rules are being used on your network. Once you have configured the accounting and reporting functionality, you can view the rule usage data that is collected using the Rule Usage tabs or the Policy Rule Hit Reports.

- **Rule Accounting** - Select whether to enable or disable rule accounting on the device.
- **Use Expanded Format for Rule Hit System Log Messages** - When enabled, the device will provide additional information in Policy Rule Hit syslog messages. For example, the additional information may include what actions may have been initiated by the rule (if any).
- **Clear Rule Usage on Port Link-Status Change** - Clears rule usage data when the port has a link-status change when a user connects or disconnects.
- **Clear Rule Usage on Role Mapping Change** - If a role-mapping is defined and traffic comes onto the device and is mapped to the defined role, then all rules in that role will have their rule hit data cleared. This option should

be enabled for Policy Rule Hit Reporting. It allows you to start a new data collection when the name of the role changes on the port, providing for a cleaner data presentation.

- **Enable Syslog Server** - For Policy Rule Hit Reporting, select this checkbox to set up the device to send syslog messages. (If the checkbox is grayed out, you must first enable the Policy Rule Hit Reporting feature in the [Policy Manager options](#).)
- **Clear Rule Usage on Interval** - Clears the rule usage data at a set interval. This option should be enabled for Policy Rule Hit Reporting because it specifies the interval at which syslog messages will be sent to the server, thereby providing data samples at even intervals. Enter the desired interval (in minutes).

If you enable any of the clear rule usage options, you must create a list of the ports on the device(s) where the clear operations will be performed, using the device [Role/Rule tab](#).

#### *Class of Service Mode Window*

Select the Class of Service mode for the device. Policy Manager supports two modes of class of service, with each mode providing a different rate limit functionality. See [Getting Started with Class of Service](#) for more information on the two modes. You can also select an option to disable rate limits on the devices you are configuring.

- **Rate Limits Disabled** - Select this option if you want rate limits disabled on the device. This means that any priority-based rate limits will not be written to the device on enforce, and any role-based rate limits will not be included in roles written to the device on enforce.
- **Role-Based Rate Limits/Transmit Queue Configuration (CoS State Enable)** - Select this mode if you want to configure role-based rate limits and transmit queues on the device. See [Defining Role-Based Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.
- **Priority-Based Rate Limits** - Select this mode if you want to configure priority-based rate limits on the device. Priority-based rate limits add to the amount of time it takes to enforce and verify roles. Once you've created your rate limits and enforced them, you may want to disable rate limits so that it takes less time to enforce. See [Defining Priority-Based Rate Limits](#) for more information.

### *Invalid Role Action Window*

Select the action you would like taken if an authenticated user is assigned an unknown or invalid role:

- **Apply Default** - Apply the port's default role to the user.
- **Deny Traffic** - Drop the packets for this user.
- **Permit Traffic** - Forward traffic with the port's assigned VID.

### *RFC3580 VLAN Authorization Status Window*

Enable or disable RFC 3580 VLAN Authorization on the device. RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. Enabling VLAN Authorization allows you to configure Authentication-Based VLAN to Role Mapping as a way to assign a role to a user during the authentication process, based on a VLAN Attribute. For more information, see [VLAN to Role Mapping](#) in the Concepts Help topic. To configure Authentication-Based VLAN to Role Mapping, use the role's [Mappings tab](#) and/or the VLAN's [General tab](#).

### *Select Devices*

1. In the **Device Selection window**, [select](#) the device(s) to which you want this configuration to apply.
2. If you would like to save this device configuration as a template, click **Save**. The Save Template window opens where you can provide a name for the template.
3. Click **Finish**.

---

**NOTE:** If you elected to enable authentication as part of the device configuration, and chose the "Select Ports to set to Inactive/Default Role" option, the [Set Authentication State to Inactive/Default Role window](#) now appears. Make your selections and click **OK** to complete the wizard.

---

## Using the Device Tabs

Configuring a device using the device tabs enables you to set up or modify the same options found in the [Device Configuration Wizard](#), but for a selected device, using the right-panel device tabs.



To configure a device using the device tabs:

1. In the left-panel Network Elements tab, select the device you want to configure. Use the right-panel tabs to configure the device.
  2. Select the [Authentication tab](#) and fill out the tab as required. Be sure to click **Apply** in any part of the tab you change.
  3. Select the [RADIUS tab](#) and fill out the tab as required.
  4. To enable [MAC Locking](#), select the [MAC Locking tab](#) and configure the options as desired.
  5. In the right panel, select the [Role/Rule tab](#) and configure a device-level role (Matrix C1 devices only) or enable Rule Accounting as desired.
  6. Select the [General tab](#) and choose your Class of Service mode.
- 

## Related Information

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)

For information on related tasks:

- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

For information on related windows:

- [Add RADIUS Authentication Server Window](#)
- [Add RADIUS Accounting Server Window](#)
- [Port Properties - Authentication Configuration Tab](#)
- [Port Usage Tab \(Device\)](#)
- [RADIUS Tab \(Device\)](#)

## How to Configure Ports

---

In Policy Manager, you can specify a port's [authentication](#) settings, as well as specify a default role for the port, freeze or unfreeze a port, enable or disable the Drop VLAN Tagged Frames and MAC Locking features, enable CEP (Convergence End Point) protocols, and set other port settings. There are two ways to configure ports:

- **Using the Port Configuration Wizard:** The Port Configuration Wizard is a series of windows that leads you through all the steps required to configure ports. You can configure a single port with the wizard, but it is even more useful for configuring multiple ports simultaneously. To configure authentication for a port in a Pre-Defined Port Group, you must use the Port Configuration Wizard.
- **Using the Port Properties Window:** You can use the Port Properties window to configure port settings for a single port.

Instructions on:

- [Using the Port Configuration Wizard](#)
- [Using the Port Properties Window](#)

### Using the Port Configuration Wizard

The Port Configuration Wizard is a series of windows that leads you through all the steps required to configure a port or ports, including setting the port mode, login settings, and default role. Use the Port Configuration Wizard to configure single or multiple ports simultaneously. You must configure and enable authentication on the device before any port authentication settings will take effect (see [How to Configure Devices](#)).

The Wizard also lets you create a *port configuration template* based on a port configuration so that you can easily configure ports that have the same configuration requirements. Once you create the template you can reuse it whenever you need that specific port configuration by simply loading the template into the Port Configuration Wizard.

1. From the menu bar, select **Tools > Port Configuration Wizard**. The Port Configuration Wizard opens.

2. This step depends on whether or not you are using a Port Configuration Template:
  - **To use a Port Configuration Wizard Template**, click the **Load** button and select the template from the list in the Open Template window. After the template has loaded, you can select **Jump to Port Selection** to [select your ports](#), or you can proceed with the wizard and [select options to configure](#) to edit the template configuration.
  - **If you are not using a using a Port Configuration Wizard Template**, proceed with selecting options to configure.

### *Select Options to Configure*

In the **Port Configuration window**, select the configurations you wish to perform:

- **Authentication**  
Lets you configure your port authentication. Refer to the NetSight Firmware Support tables for information on the authentication types supported by each device type. For more information on the different types of authentication, see [Authentication Types](#).
- **Default Role & Drop VLAN Tagged Frames** - Lets you assign a default role and enable the Drop VLAN Tagged Frames feature on the ports. 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. See [Default Role](#) for more information. If you set a default role for the ports, it is recommended that you enable the Drop VLAN Tagged Frames feature. This feature lets you set the ports so that any packet already tagged with a VLAN coming into the ports will be dropped. See [Drop VLAN Tagged Frames](#) for more information.
- **Frozen Status** - Enables you to "lock" the ports so that no one can accidentally reconfigure its sensitive attributes. See [How to Freeze/Unfreeze a Port](#) for more information.
- **MAC Locking** - Lets you enable [MAC Locking](#) on ports, if the device on which the port is located supports it.
- **Disable Traffic Classification Types** - Lets you create a list of rule types that will be disabled on the ports.
- **Egress Policy Status** - Lets you enable Egress Policy on ports, if the device on which the port is located supports it.

- **RFC3580 VLAN Authorization** - Lets you enable or disable RFC 3580 VLAN Authorization on the ports and specify an egress state.
- **Tagged Packet VLAN to Role Mapping** - Lets you configure Tagged Packet VLAN to Role mappings on the ports. These mappings provide a way to let ports assign a role to network traffic, based on a VLAN ID.
- **MAC/IP to Role Mapping** - Lets you configure MAC or IP to role mappings on the ports. These mappings provide a way to let ports assign a role to an end station based on its source MAC or IP address.

### *Configure Settings*

The sequence of windows you see next depends on the selections you made in the Port Configuration window.

**NOTE:** Each window provides the option to use the current configuration on the port(s), or set a new configuration. If you select **Use Current Configuration on Port(s)**, the default settings in the window are visible, but are unavailable for entry or editing. Keep in mind that these values do not necessarily reflect the current settings on the port.

### Port Authentication Configuration Window

Select the authentication parameters you wish to configure. The selections you make here will determine the other Authentication configuration windows you will see.

- **Shared Settings**
  - **Port Mode (802.1X , MAC, Web-Based, CEP, Quarantine, Auto Tracking)** - Defines whether or not end users are required to authenticate, and how unauthenticated traffic will be handled. See [Port Mode](#) for more information.
  - **Hold Time (802.1X, MAC, Web-Based)** - (Also known as Quiet Period in web-based and MAC authentication.) Amount of time (in seconds) authentication will remain timed out after the specified Timeout Number has been reached.
  - **Automatic Re-Authentication (802.1X, MAC)** - Lets you enable the periodic automatic re-authentication of logged-in users.
  - **Authenticated User Counts (802.1X, MAC, Web-Based)** - The number of users that can be actively authenticated or have authentications in progress at one time on a port. This option is for ports on devices with Multi-User as their configured authentication type.

- **802.1X Settings**
  - **Authentication Request Period** - How often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user.
  - **User Timeout** - The amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user.
  - **Authentication Server Timeout** - If a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out.
  - **Port Handshake Requests** - The number of times the device tries to finalize the authentication process with the user, before the authentication request is considered invalid and authentication fails.
- **Web-Based Settings**
  - **Timeout Number** - Number of times a user can attempt to log in before authentication fails and login attempts are not allowed.
- **CEP Settings**
  - **CEP Protocol Enable** - Lets you enable various CEP (Convergence End Point) protocols on ports, if the device on which the port is located supports CEP. See [How to Configure CEP](#) for more information.

### Port Mode Window (802.1X, MAC, Web-Based, CEP, Quarantine, Auto Tracking)

Specify the desired port mode for ports. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on a port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to a port's default role or discarded). See [Port Mode](#) for a complete description of each port mode.

---

**NOTES:** If you set the ports' Authentication Behavior to Active, it is recommended that you enable the [Drop VLAN Tagged Frames](#) feature on the ports.

For Single User 802.1X or 802.1X+MAC authentication: If you set port mode to Active/Default Role, then the selected default role will be automatically set on the configured ports. If you set port mode to Active/Discard, then any default role assigned to the ports will be automatically cleared.

---

In addition, the Port Mode window provides checkboxes that allow you to disable a specific authentication type at the port level. If the device is only configured with one authentication type, selecting the corresponding checkbox will result in the port Authentication Behavior being set to Inactive.

**NOTES:** — For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port will not be able to authenticate via 802.1X or MAC. The port will behave as if Inactive/Default Role is the selected port mode.

— For Multi-User Web-Based authentication with Active/Discard as the selected port mode: The "Disable Web-Based authentication for specified port(s)" checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

### Hold Time Window (802.1X, MAC, Web-Based)

Enter the amount of time (in seconds) authentication will remain timed out after the specified Timeout Number has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

### Authentication Request Period Window (802.1X)

Enter how often (in seconds) the device should query the port to see if there is a new user on it. Valid values are 1-65535. The default is 30.

### User Timeout Window (802.1X)

Enter the amount of time (in seconds) the device should wait for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

### Authentication Server Timeout Window (802.1X)

Enter the amount of time (in seconds) the device should wait for a response from the authentication server before timing out, if a user is found on the port. Valid values are 1-300. The default is 30.

### Port Handshake Requests Window (802.1X)

Enter the number of times the device should try to finalize the authentication process with the user, before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

### Automatic Re-Authentication Window (802.1X, MAC)

Enable or disable the automatic re-authentication feature by setting the Re-Authentication Status to Active (enabled) or Inactive (disabled). This specifies whether or not the device should periodically repeat the authentication process for logged-in users on this port. If you activate automatic re-authentication, specify how often this should occur (Re-Authentication Frequency), in seconds. Valid values are 1-2147483647. The default is 3600.

### Authenticated User Counts Window (802.1X, MAC, Web-Based)

This option is for ports on devices with Multi-User as their configured authentication type. Enter the maximum number of users that can be actively authenticated or have authentications in progress at one time on the specified ports. The maximum number allowed varies for different port types. If you set this value below the current number of users on the ports, end user sessions exceeding that number will be terminated. If you have selected MAC as a Multi-User authentication type, enter the maximum number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of allowed MAC users cannot exceed the number of allowed users. If you set this value below the current number of users, end user sessions exceeding that number will be terminated.

### Timeout Number Window (Web-Based)

Enter the number of times a user can attempt to log in before authentication times out and further login attempts are not allowed. Valid values are 1-2147483647. Zero is not allowed. The default is 2.

### CEP Protocol Enable Window

Enable or disable various CEP protocols for the ports being configured. The table lists all the CEP protocols currently supported by Policy Manager. Use the checkboxes (or the Enable All and Disable All buttons) to enable or disable the desired CEP protocols. You must configure and enable CEP on the device in addition to configuring CEP on the ports (see [How to Configure Devices](#)).

### Default Role Window

Use the drop-down list to select a default role for the ports. If you already set the ports' Authentication Behavior to Active and specified a default role in the Port Mode window, then this panel will be disabled. Select the **Clear the current default role** option to set the default role back to <None>. If you set a default role

for the ports, it is recommended that you enable the [Drop VLAN Tagged Frames](#) feature.

### Drop VLAN Tagged Frames Window

Choose whether or not you want packets already tagged with a VLAN to be dropped from the ports. Usually you would have this enabled for user ports and disabled for interswitch ports. See [Drop VLAN Tagged Frames](#) for more information.

---

**WARNING:** Enabling this feature on an interswitch or backplane port is likely to result in loss of contact with devices connected through the port.

---

### Frozen Status Window

Enables you to "lock" the ports so that no one can accidentally reconfigure its sensitive attributes. Select either the **Set Frozen** or **Clear Frozen** option.

### MAC Locking Window

Enable or disable [MAC Locking](#) for the ports being configured. You can also set the maximum number of MAC addresses that are allowed to be locked dynamically or statically on a port. Use the Static Locked MAC Addresses table to create a list of locked MAC addresses, so that the ports only accepts traffic from those MAC addresses. Click **Add** to open the Enter Static Locked MAC window, where you can enter a MAC address to add to the list. Click **Remove** to remove a selected entry from the Locked MAC Addresses list.

### TCI Overwrite Window

Enable or disable TCI Overwrite functionality for the ports being configured. Enabling TCI Overwrite causes the VLAN or class of service tag in a received packet to be overwritten by the VLAN (access control) and class of service characteristics defined in the port's current or default role. If there is no role assigned to the port, the port uses any static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port.

TCI Overwrite is required for some devices for Tagged Packet [VLAN to Role Mapping](#), and can be enabled either here at the port level, or for an individual role in the role's [General tab](#).



## Disable Traffic Classification Types Window

Create a list of traffic classification rule types that will be disabled on the ports. For example, you can disable the VLAN ID traffic classification type to disable Tagged Packet VLAN to Role Mapping on the ports you are configuring. Click **Add** to open the [Traffic Classification Type wizard](#) where you can select the rule type you want to add to the list, or click **Add All** to add all rule types to the list. Adding all rule types would disable all traffic classification on the port, and the role's default class of service and/or default access control would take effect. Click **Remove** to remove selected rule types from the list.

## Egress Policy Status Window

Enable or disable Egress Policy for the ports being configured. Egress policy can be used in scenarios where policy may not be in force at the user edge throughout the entire network. For example, a policy can be created that prevents users from running unauthorized Apache web servers. If an end user has an Apache server running on their end-system (where policy is in use), an egress policy could prevent another end-system (where policy is not in use) from accessing that end-system as an HTTP server, by dropping HTTP queries destined to that end user. Egress policy works in conjunction with the ingress policy configured for the port, in that the same ingress policy rules will be applied to the traffic egressing the port, with the exception of rules that specify a source or destination address. In this case, the ingress rules will still be used, but the direction of the rule will be inverted on egress. For example, an ingress MAC Address Source rule will match the destination MAC address of the frame on egress. If you enable egress policy, you must also enable TCI Overwrite.

## RFC3580 VLAN Authorization Window

Enable or disable RFC 3580 VLAN Authorization for the ports being configured. VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy, will tag packets with the VLAN ID.
- ports on devices that do support policy and also support [Authentication-Based VLAN to Role Mapping](#), will classify packets according to the role that the VLAN Attribute maps to.

You can also modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

The current egress settings for the port are displayed in the [VLAN Oper Egress column](#) in the End User Sessions table on the Port Usage tabs.

### Tagged Packet VLAN to Role Mapping Window

Use this window to either remove all port-level mappings from the selected ports, or create a list of mappings to append to the ports. Click **Add** to open the VLAN to Role Mapping Selection View, where you can select a VLAN and map it to a role. Click **Remove** to remove selected mappings from the list. You must have the Port Level Role Mappings feature enabled in Policy Manager for these mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored. Mappings will not be added or removed to or from frozen ports. You must first clear the frozen state on a port in order to add or remove a mapping.

---

#### **NOTES: TCI Overwrite Requirement**

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a COS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingress with.

If supported by the device, you can enable TCI Overwrite on a per-port basis in the [Port Properties window General tab](#), or for an individual role in the role's [General tab](#). The stackable devices support rewriting the CoS values but not the VLAN ID.

---

### MAC/IP to Role Mapping Window

Use this window to either remove all port-level mappings from the selected ports, or create a list of mappings to append to the ports. Click **Add** to add a MAC or IP to Role Mapping to the list. Click **Remove** to remove selected mappings from the list. You must have the Port Level Role Mappings feature

enabled in Policy Manager for these mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored. Mappings will not be added or removed to or from frozen ports. You must first clear the frozen state on a port in order to add or remove a mapping.

---

**WARNING:** Enforcing port-level MAC or IP to Role mappings could potentially remove rules created by NetSight Automated Security Manager (ASM) as an intrusion detection response.

---

### *Select Ports*

In the **Port Selection window**, you can select the ports you want to include or exclude from this configuration.

1. In the Devices field, expand the folders and select the ports you want to configure.
2. Click **Add Include** to include the selected ports in this configuration or click **Add Exclude** to exclude the ports from the configuration. For example, you may want to configure all your 10/100 ports except printer ports. You would select the Pre-Defined Port Group of 10/100 ports and click Add Include. Then you would select a User-Defined Port Group of printer ports and click Add Exclude.
3. To remove a port from the Include Ports or Exclude Ports fields, select the port and click **Remove**.
4. If you would like to save this device configuration as a template, click **Save**. The Save Template window opens where you can provide a name for the template.
5. Click **Finish**. The settings will take effect.

---

**NOTE:** You must configure and enable authentication on the device before any port authentication settings will take effect (see [How to Configure Devices](#)).

---

## Using the Port Properties Window

Configuring a port using the Port Properties window accomplishes the same things as the Port Configuration Wizard, but also enables you to view the current configuration on the port. To configure authentication for a port in a Pre-Defined Port Group, you must use the [Port Configuration Wizard](#).

- [Assigning Default Roles to Ports](#)
- [Clearing Default Roles from Ports](#)
- [Disabling Traffic Classification Rules on Ports](#)
- [Enabling CEP Protocol](#)
- [Enabling Drop VLAN Tagged Frames](#)
- [Freezing/Unfreezing Ports](#)
- [Locking MAC Addresses to Ports](#)
- [Setting Port Authentication](#)
- [Terminating a Session](#)

### *Assigning Default Roles to Ports*

You can assign a default role to a single port, or to multiple ports. If you set a default role for a port, it is recommended that you enable the [Drop VLAN Tagged Frames](#) feature.

---

**NOTE:** Setting a default role on an ExtremeWireless Wireless Controller port that is not yet a VNS, creates a new VNS on the wireless controller.

---

### Single Port

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [General tab](#) (in the top row of tabs).
3. Select the [Role Status sub-tab](#). You can view the default role for the port. Click the **Select** button to select a new default role. This opens the [Selection View](#), where you can select an existing role. Select the **Clear the current default role** option to set the default role back to <None>. Click **OK**.

### Multiple Ports

There are two ways to assign a default role to multiple ports:

- Using the Default Role Window in the [Port Configuration Wizard](#). Using the wizard is most useful when you want to do other port configuration tasks as well.
- Assigning the default role to a device, a device group, or a pre-defined or user-defined port group, as follows:

1. **For a device or device group:** in the left-panel Network Elements tab, right-click the device or device group that includes the ports to which you want to assign the default role, and select **Set Default Role** from the menu.  
**For a port group:** in the left-panel Port Groups tab, right-click the group for the ports to which you want to assign the default role, and select **Set Default Role** from the menu.
2. In the [Selection View](#), select the role you want to assign as the default. Click **OK**.

### *Clearing Default Roles from Ports*

You can clear the default role from a single port, or from multiple ports.

#### Single Port

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [General tab](#) (in the top row of tabs).
3. Select the [Role Status sub-tab](#). Click the **Select** button to select a new default role. This opens the [Selection View](#), where you can select the **Clear the current default role** option to set the default role back to <None>.
4. Click **OK**.

---

**NOTE:** If you are replacing the current default role with another one, you don't need to clear the current default role. Selecting the new default role and clicking **OK** clears the previous default role automatically.

---

#### Multiple Ports

There are two ways to clear the default role from multiple ports:

- Using the **Clear the current default role** option on the Default Role Window in the [Port Configuration Wizard](#). Using the wizard is most useful when you want to do other port configuration tasks as well.
- Clearing the default role from a device, a device group, or a port group, as follows:
  1. **For a device or device group:** in the left-panel Network Elements tab, right-click the device or device group that includes the ports to which you want to assign the default role, and select **Set Default Role** from

the menu.

**For a port group:** in the left-panel Port Groups tab, right-click the group of ports to which you want to assign the default role, and select **Set Default Role** from the menu.

2. In the [Selection View](#), select the **Clear the current default role** box.
3. Click **OK**.

---

**NOTE:** If you are replacing the current default role with another one, you don't need to clear the current default role. Selecting the new default role and clicking **OK** clears the previous default role automatically.

---

### *Disabling Traffic Classification Rules on Ports*

You can create a list of traffic classification rule types to disable on a port using the Port Properties window. For example, you could disable the VLAN ID traffic classification type, which would disable Tagged Packet VLAN to Role Mapping on the port.

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [General tab](#) (in the top row of tabs).
3. Select the [Disabled Traffic Classification Types sub-tab](#).
4. Use the **Add** button to open the [Traffic Classification Type wizard](#) and create the list of rules you want to disable.

### *Enabling CEP Protocol*

You can enable and disable CEP protocols for a specific port using the [CEP Access sub-tab](#) on the Port Properties window Authentication Configuration tab. (You can enable CEP protocols for multiple selected ports using the [Port Configuration wizard](#).) In order for CEP to take effect on a port, it must also be enabled at the device level. You can do this using the [Device Configuration wizard](#), or the device [Authentication tab](#). See [How to Configure CEP](#) for more information.

### *Enabling Drop VLAN Tagged Frames*

When the Drop VLAN Tagged Frames feature is enabled, any packet already tagged with a VLAN coming into the port will be dropped. Usually you would enable this for user ports, and disable it for interswitch ports.

---

**WARNING:** Enabling this feature on an interswitch or backplane port is likely to result in loss of contact with devices connected through the port.

---

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [General tab](#) (in the top row of tabs).
3. Select the [Drop VLAN Tagged Frames sub-tab](#). In this tab, select the Enable button.
4. Click **Enforce** on the toolbar, review the effects of enforcing in the [Enforce Preview window](#) if it is enabled, then click **Enforce** on that window.

### *Freezing/Unfreezing Ports*

See [How to Freeze/Unfreeze a Port](#).

### *Locking MAC Addresses to Ports*

See [How to Lock MAC Addresses to Ports](#).

### *Setting Port Authentication*

You can configure authentication settings for a selected port in the Port Properties window. Before any port authentication settings will take effect, you must configure and enable authentication on the device (see [How to Configure Devices](#)).

---

**NOTE:** In order to configure authentication for a port in a Pre-Defined Port Group, you must use the [Port Configuration Wizard](#).

---

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [Authentication Configuration tab](#) (in the top row of tabs).
3. Use the sub-tabs to make changes as required.

### *Terminating a Session*

Terminating a session causes the port to be re-initialized. The user loses the access rights of the current role on the port and reverts to the access rights

specified for unauthenticated behavior on the port, until he or she authenticates again.

With web-based authentication, the user must log in again using the authentication web page after the port re-initializes. With 802.1X authentication on Windows 2000, the user is prompted to log in again after the port re-initializes. With 802.1X authentication on the Windows XP platform, the user is automatically reauthenticated immediately after the port re-initializes, and no login prompt occurs.

You can terminate an authenticated session on a single port in the Port Properties Window or multiple ports in the Port Usage tab for a device, a device group, or a port group. If sequential multiple ports are selected, only authenticated sessions whose [Terminate Cause](#) is "Not Applicable" are affected. You cannot terminate sessions on frozen ports and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface).

---

**NOTE:** For 802.1X authentication on the Windows XP platform, if you terminate a user's session, the user is automatically reauthenticated, unless there has been a policy change or a change in the user's authentication status (e.g., the user has been removed from the authentication list).

---

## Single Port

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Properties** from the menu. In the Port Properties window, select the [Port Usage tab](#) (in the top row of tabs).
3. Select the [End User Sessions sub-tab](#). You must click **Retrieve** to display the port information in the table.
4. Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate a session on a [frozen port](#) and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface).
5. Click **Yes** to confirm that you want to terminate.



## Multiple Ports

Select the right panel Port Usage tab for one of the following left-panel selections, depending on the ports whose session(s) you want to terminate:

- [Device](#)
  - [My Network/All Devices Folder](#)
  - [Device Group](#)
  - [Port Group](#)
- 

## Related Information

For information on related concepts:

- [Port Mode](#)
- [MAC Locking](#)

For information on related tasks:

- [Authentication Configuration Guide](#)
- [802.1X Authentication Configuration Supplement](#)

For information on related windows:

- [Port Properties - Authentication Configuration Tab](#)
- [Port Properties - Port Usage Tab](#)
- [Port Properties - General Tab](#)

## How to Create a Network Resource

---

Network Resource groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. You create a network resource group by defining a list of MAC or IP addresses for the resources that you want included in the group.

In addition, you can use [Network Resource Topologies](#) to define a different resource list for different groups of devices in your domain. This enables you to set up network resource access based on the location where end users authenticate.

Once a network resource group has been defined, you can associate it with an [Automated service](#) (see [How to Create a Service](#) for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource address in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

You can also create Global Network Resources which will be shared between all your domains and can be used by global automated services. Network Resource Topologies are not available for Global Network Resources.

---

**TIP:** The Policy Manager [Demo.pmd file](#) contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers.

---

### How to Create a Network Resource

1. From the Edit menu, select Network Resources Configuration. The Network Resource Configuration window opens.
2. Right-click the Network Resources folder and select **Create Network Resource**. A New Network Resource item is created in the left panel in a highlighted box. (If you want to create a Global Network Resource, click on the Global Network Resources folder.)
3. Type the resource name in the highlighted box.
4. In the right-panel General tab, use the **Edit** button to add a description of the network resource, if desired.

5. Select the network resource Type:
  - Layer 2 MAC - Define a group of network resources using MAC addresses.
  - Layer 3 IP - Define a group of network resources using IP addresses.
6. Select the appropriate network resource topology. [Network Resource Topologies](#) are used to divide the devices in a domain into groups called islands. You can then define a unique resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate. If you are not using topologies to group your devices, select the Domain Wide topology, which contains just one island for all your domain devices.
7. For each topology island included in the selected topology, you will see a tab where you can list the resources for that specific island. Use the address field (MAC or IP, depending on the selected type) to add a new resource to the list. Use the Copy and Paste buttons to copy a resource address from one island and paste it into another island.

Once a network resources group has been created and defined, it can be associated with an Automated service (see [How to Create a Service](#) for more information).

---

**TIP:** To quickly view what resources belong to a device, select the device (not the device type folder) in the Device Support tab for the automated service or the role that includes that service.

---

## How to Create a Network Resource Topology

1. From the Edit menu, select Network Resources Configuration. The Network Resource Configuration window opens.
2. Right-click the Network Resource Topologies folder and select **Create Network Resource Topology**. A New Network Resource Topology item is created in the left panel in a highlighted box.
3. Type the topology name in the highlighted box.
4. Expand the topology to see the Default Island, which contains all the devices in the domain.
5. Right-click on the topology and select **Create Network Resource Island**. Type in the island name in the highlighted box. Use this step to create all the islands for this topology.

6. Right-click on an island and select **Modify Island Device Membership** to open the Island Device Membership window where you can move devices from the Default Island to the islands you just created. Click **OK**.
7. Set any island as the [Default] island for new devices that are added to the domain by right-clicking the island and selecting **Set as Default Island for New Devices**.

The Network Resource Topology will now be available for selection when you create your network resources.

---

### **Related Information**

For information on related tasks:

- [How to Create a Service](#)

For information on related windows:

- [General Tab \(Network Resource Group\)](#)

## How to Create a Port Group

---

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

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

Policy Manager also provides you with Pre-Defined Port Groups which are automatically populated according to port characteristics. See [Pre-Defined Port Groups](#) for more information.

Instructions on:

- [Creating a Port Group](#)
- [Adding Ports to a Port Group](#)
- [Removing Ports from a Port Group](#)

### Creating a Port Group

1. In the left panel, click the Port Groups tab.
2. Right-click on the User-Defined Port Groups folder and select Create Port Group. This expands the folder and creates a "New Port Group" item.
3. Type the port group name in the highlighted box and press **Enter**.
4. In the right panel, click the **Edit** button and enter a description of the port group, if desired.
5. To add ports to the group, click the **Add/Remove Ports** button and use the [Add/Remove Ports window](#) to add ports.

### Adding Ports to a Port Group

You can add a port to a port group by right-clicking on the port and selecting Add to Port Group(s) from the menu.

You can also add ports directly from the port group:

1. Select the left-panel Port Groups tab. Expand the User-Defined Port Groups folder and select a port group.
2. You can either right-click the port group and select Add/Remove Ports from the menu, or click the Add/Remove Ports button in the right-panel Ports tab.
3. In the Add/Remove Ports window, select the ports you want to put into the port group, and click **Add**.
4. Click **OK**.

Alternatively, you can drag and drop a single port from a list of ports in the left panel (e.g., the list that results from expanding another port group) to the port group, or copy and add single or multiple ports from the right-panel device [Details View tab](#) (on the Network Elements tab) to the port group. To make multiple selections in the right panel, hold down **Ctrl** (for non-sequential ports) or **Shift** (for sequential ports) while selecting the ports.

## Removing Ports from a Port Group

This procedure applies to user-defined port groups.

1. In the left-panel Port Groups tab, right-click the port group from which you wish to remove a port, and select Add/Remove Ports.
2. In the Add/Remove Ports window, select the ports you want to remove from the port group, and click **Remove**.
3. Click **OK**.

Alternatively, you can right-click a single port under the port group in the left panel or multiple ports in the right-panel Ports tab, and select **Remove Port(s) from Group**.

---

## Related Information

For information on related windows:

- [Add/Remove Ports Window](#)

## How to Create a Quarantine Role

---

The Quarantine role is a highly restrictive role used to isolate users and restrict network access.

The Quarantine role is used in conjunction with the Extreme Networks Intrusion Prevention System (IPS) and the NetSight Automated Security Manager to create an automatic response to threats detected on the network. Once the Quarantine role has been enforced to the network, and both the Extreme Networks IPS and the Automated Security Manager are properly configured, this role can be automatically set as the default role on any port where a threat has been detected. Normally, roles are applied to ports via authentication. In this case however, the Automated Security Manager determines a network threat, identifies the responsible port, and applies the Quarantine role to the port.

The Quarantine role can also be used when configuring [Quarantine Authentication](#) in Policy Manager, and by the NetSight NAC Manager assessment functionality. You can also set the Quarantine role as a port's default role through Policy Manager if, for example, you have modified the role to provide some limited access and you want to use it as a "guest" role.

The Policy Manager default domain includes the Quarantine role. However, if you add a new domain, you will need to create the Quarantine role. For information on how to create a role, see [How to Create a Role](#).

After you have created the role, you can modify the role's default class of service and access control settings, and make changes to the role's services and rules using the right-panel tabs, just like any other role. If you make any changes to the Quarantine role, keep in mind that the role may be used by other applications and should remain highly restrictive in nature.

### Instructions on:

- [Modifying the Quarantine Role](#): Use the right-panel tabs to modify the Quarantine role's default values and add or remove services.
- [Setting the Quarantine Role as the Default Role on a Port](#): Use the right-panel General tab or the Port Configuration wizard to set the Quarantine role as a default role on a port.

## Modifying the Quarantine Role

Once you've created a Quarantine role, you can change its characteristics by selecting the role in the Policy Manager's left panel and using the associated tabs in the right panel.

**NOTE:** Because it is used by the Automated Security Manager, you cannot rename the Quarantine role.

### *Modifying Default Values*

Use the [General tab](#) to change the Quarantine role's default class of service and default access control settings, and to add or edit a description.

1. Select the Quarantine Role in the left-panel Roles tab.
2. In the right-panel General tab, select the desired default class of service and default access control settings.
3. If desired, add or edit the role's description.
4. Be sure to perform an [Enforce](#) to write the new Quarantine role to the devices.

### *Adding/Removing Services*

Use the [General tab](#) to add or remove services to the Quarantine role.

1. Select the Quarantine Role in the left-panel Roles tab.
2. In the right-panel General tab, click **Add/Remove Services**. This opens the [Add/Remove Services window](#).
3. Make sure the Quarantine role is displayed in the Role selection box.
4. In the Groups and Services panel, select the services and/or service groups you wish to add to the role, and click **Add**. To remove services, select them in the Selected Services panel and click **Remove**.

**NOTE:** Policy Manager checks for rule conflicts when more than one service is added. See [Conflict Checking](#) for more information.

5. Click **OK**.
6. Be sure to perform an [Enforce](#) to write the new Quarantine role to the devices.



## Setting the Quarantine Role as the Default Role on a Port

When the Automated Security Manager detects a threat on the network, it automatically assigns the Quarantine role as the default role on that port. However, there may be circumstances when you would like to use Policy Manager to assign the Quarantine role as the default role on one or more ports. For example, if you have modified the Quarantine role to provide limited access, you may want to use it as the default role for guest users on your network.

The Quarantine role is assigned as a default role just like any other role. Refer to [Assigning Default Roles to Ports](#) for instructions.

---

### Related Information

For information on related tasks:

- [Assigning Default Roles to Ports](#)

For information on related windows:

- [Add/Remove Services Window](#)
- [General Tab \(Role\)](#)

## How to Create a Role

---

A [role](#) is a policy profile consisting of a set of network access services that you can apply at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates.

There are two ways to create a role:

- **Using the Role Wizard:** The Role Wizard is a series of windows that leads you through all the steps for creating a role, including the optional selection and enabling of default access control (default VLAN) and/or class of service for the role, as well as specifying the existing services and service groups that will apply to the role. You can also create new services in the Role Wizard, which encompasses the [Service Wizard](#). If you want to associate a role with a default access control and/or class of service only, without any services, it may be handier to create the role name with the **Create a Role** menu option, and use the role General tab to set the defaults.
- **Using the Role Tabs:** Creating a role using the role tabs consists of creating a name for the role with the **Create Role** menu option, then defining its characteristics (default class of service, default access control, and/or services) using the role's right-panel tabs. It accomplishes the same things as the Role Wizard, but enables you to do only those parts of the procedure you want to do, when you want to do them. You might also use this method if you are creating a role for which there is default class of service and/or access control, but no services.

If you want to change the characteristics of a role, you can select the role in the left panel and use the right-panel tabs to modify it.

Instructions on:

- [Using the Role Wizard](#)
- [Using the Role Tabs](#)
- [Modifying a Role](#)
- [Deleting a Role](#)

### Using the Role Wizard

The Role Wizard is a series of windows that leads you through all the steps for creating a role, including the optional selection and enabling of default access

control and/or class of service for the role, as well as specifying the existing services and service groups that will apply to the role.

1. In the Policy Manager left panel, click the Roles tab.
2. Right-click on the Roles folder and select Role Wizard.
3. In the **Name window**, enter the name of the role. The name can be up to 64 characters in length, and special characters are allowed, with the exception of colons (:) and semicolons (;). Duplicate names are not allowed, regardless of case. For example, if you already have a role "Faculty" and you attempt to name the new role "Faculty" or "faculty," Policy Manager will create the role, but with the name "New Role," or "New Role(n)" (where "n" is the sequence number, if there is more than one "New Role"). You can then rename the new role. After entering the name, click **Next**.
4. In the **Default TCI Overwrite window**, enable or disable TCI Overwrite functionality for the role. Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this role or any of its rules to overwrite the VLAN or class of service (CoS) tag in a received packet if that packet has already been tagged with VLAN or CoS information. If TCI Overwrite is not enabled, tagged packets will egress using the TCI data they already contain. You can also enable TCI Overwrite on a per-port basis in the [Port Properties General Tab](#), as well as on a per-rule basis in the [Rule General Tab](#). Click **Next**.
5. In the **Default Access Control window**, you can assign default access control to the role, if desired. Default access control will be applied to traffic not identified specifically by the set of access services contained in the role. Choose one of the following options, then click **Next**.
  - **None** - No default access control specified.
  - **Permit (Using Existing Port VLAN)** - Allows traffic to be forwarded with the port's assigned VID.
  - **Deny Traffic** - Traffic will be automatically discarded.
  - **Contain to VLAN** - If you want to contain traffic for this role, select this option, then select the appropriate VLAN from the list or create a new one, if desired.

Click **Next**.

6. In the **Default Class of Service window**, you can assign a default class of service to the role, if desired. Select the desired class of service in the list. If the priority for the class of service includes a priority-based rate limit, this

will be noted in the class of service name (see [How to Create a Class of Service](#) for more information). Click **Next**.


---

**NOTES:** If you select a CoS that is associated with a ToS/DSCP value, the ToS/DSCP value will be ignored. This is because ToS/DSCP rewrite works only for certain IP ToS classification rules, not as a role default. See [ToS/DSCP Rewrite](#) for more information.

Once a rate limit is applied to a port, that port's bandwidth will be rate limited, even if the default or authenticated role that applied the rate limit is no longer associated with the port.

---

7. In the **Default Actions - Acct/Sec/Mirror window**, you can specify the default accounting and security actions for the role. These actions are applied if the traffic originating from users assigned to this role does not match any rules that explicitly prohibit these actions. Select the desired actions and click **Next**.
- **System Log** - When this option is enabled, a syslog message is generated as long as no matching rules specify that sending a syslog message is prohibited (that is, the rule's system log action is set to "Prohibited" on the [Rule General tab](#)). When the option is disabled, the system log setting is ignored.
  - **Audit Trap** - When this option is enabled, an audit trap is generated as long no matching rules specify that sending an audit trap is prohibited (that is, the rule's audit trap action is set to "Prohibited" on the [Rule General tab](#)). When the option is disabled, the audit trap setting is ignored.
  - **Disable Port** - When this option is enabled, the port is disabled as long no matching rules specify that disabling the port is prohibited (that is, the rule's disable port action is set to "Prohibited" on the [Rule General tab](#)). Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#). When the option is disabled, the disable port setting is ignored.
  - **Traffic Mirror** - Use the drop-down list to specify port groups where [mirrored traffic](#) will be sent for monitoring and analysis. You will see an option below to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to a Application Analytics appliance. The Application Analytics appliance only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and

appliance. By default this number is set to 10, but can be changed by clicking on the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.

8. In the **Role Services** window, [select](#) the services you want to apply to this role. If you want to [create a new service](#) to add to the list before selecting, click **New**. Click **Finish**.

---

**NOTE:** Policy Manager checks for rule conflicts when more than one service is added. See [Conflict Checking](#) for more information.

---

9. [Enforce](#) to write the new information to the devices.

Now that you have created the role, you can:

- Add a description to the role on the right-panel General tab.
- [Assign the role as the default role for a port](#)
- [Modify the role](#)

## Using the Role Tabs

Creating a role using the role tabs consists of creating a name for the role, then using the right-panel role tabs to specify the characteristics of the role (default class of service, default access control, and/or services).

1. In the Policy Manager left panel, select the Roles tab.
2. Right-click the Roles folder, and select Create Role.
3. Type the role name in the highlighted box. The name can be up to 64 characters in length, and special characters are allowed, with the exception of colons (:) and semicolons (;). Duplicate names are not allowed, regardless of case. For example, if you already have a role "Faculty" and you attempt to name the new role "Faculty" or "faculty," Policy Manager will create the role, but with the name "New Role," or "New Role(n)" (where "n" is the sequence number, if there is more than one "New Role"). You can then rename the new role. Press **Enter** after you've entered the name. (If you don't press **Enter**, the name will remain "New Role.")
4. Select the role in the left panel, and the [General tab](#) in the right panel. Use the General tab to add a role description, enable TCI Overwrite, and set the role's default actions (including access control and class of service).

5. In the Services section in the [General tab](#), click the **Add/Remove Services** button to add services to the role. This opens the role [Add/Remove Services](#) window.

---

**NOTE:** Policy Manager checks for rule conflicts when more than one service is added. See [Conflict Checking](#) for more information.

---

6. To add a VLAN to the Role's Egress list, select the role and use the [VLAN Egress tab](#) in the right panel.
7. To configure MAC, IP, and VLAN to role mapping lists for the role, select the role and use the [Mappings tab](#) in the right panel.
8. Now that you have created the role, you can:
  - [Assign the role as the default role for a port](#)
  - [Modify the role's characteristics](#)
9. [Enforce](#) to write the new information to the devices.

## Modifying a Role

Once you've created a role, you can change its characteristics by selecting the role in the Policy Manager's left panel and using the associated tabs in the right panel.

Instructions on:

- [Adding Services to Roles](#)
- [Modifying a Role's Default Class of Service](#)
- [Modifying a Role's Default Access Control](#)
- [Modifying a Role's Description](#)
- [Modifying a Role's Ports](#)
- [Removing Services from Roles](#)

### *Adding Services to Roles*

There are two ways to add services to roles:

- During the creation of a role, in the Role Wizard's Role Services window. See [Creating a Role Using the Role Wizard](#) for instructions.
- Accessing the [Add/Remove Services window](#) from the role General tab. Use this method to add services to existing roles. Instructions are below.

1. Select the left panel Roles tab and expand the Roles folder. Select the role to which you want to add services, then select the [General tab](#) in the right panel.
2. Click **Add/Remove Services**. This opens the [Add/Remove Services window](#).
3. Make sure the role to which you wish to add services is displayed in the Role selection box.
4. In the Groups and Services panel, [select](#) the services and/or service groups you wish to add to the role, and click **Add**. To remove services, select them in the Selected Services panel and click **Remove**.

---

**NOTE:** Policy Manager checks for rule conflicts when more than one service is added. See [Conflict Checking](#) for more information.

---

5. If you wish, you can select another role, and add or remove services from it.
6. Click **OK**.
7. [Enforce](#) to write the new information to the devices.

### *Removing Services from a Role*

1. Select the left panel Roles tab and expand the Roles folder.
2. Select the role from which you want to remove services, then select the [General tab](#) in the right panel.
3. Click **Add/Remove Services**. This opens the [Add/Remove Services window](#).
4. Make sure the role from which you wish to remove services is displayed in the Role selection box.
5. In the Selected Services panel, [select](#) the services and/or service groups you wish to remove from the role, and click **Remove**. To add services, select them in the Groups and Services panel and click **Add**.
6. If you wish, you can select another role, and remove services from or add services to it.
7. Click **OK**.
8. [Enforce](#) to write the new information to the devices.

### *Modifying a Role's Default Class of Service*

Use the role's [General tab](#) to change its default class of service settings. Be sure to [enforce](#) to write the new information to the devices.

### *Modifying a Role's Default Access Control*

Use the role's [General tab](#) to change its default access control. Be sure to [enforce](#) to write the new information to the devices.

### *Modifying a Role's Description*

You can edit the description for the role on the role's [General tab](#). Click **Save** to save the change to the database.

### *Modifying a Role's Ports*

You can view the ports for which a role is the default role on the role's [Ports tab](#). You can then select a port and use the **Port Properties** button to open the Port Properties window, where you can change the default role for a port or make changes to the port settings themselves.

1. In the Policy Manager left panel, click the Roles tab.
2. Expand the Roles folder if necessary, and select the role whose ports you want to view.
3. In the right panel, select the Ports tab.
4. Click **Retrieve** to update the table with the most current information.
5. Select a port to which you want to make changes.
6. Click **Port Properties**. This takes you to the Port Properties window where you can:
  - *Modify the default role for the port:* Use the [General tab](#) (Role Status sub-tab).
  - *Modify the port's authentication settings:* Use the [Authentication Configuration tab](#).
7. [Enforce](#) to write the new information to the devices.



## Deleting a Role

1. Select the left panel Roles tab and expand the Roles folder.
  2. Right-click the role you want to delete, and select **Delete**.
  3. Click **Yes** to confirm. After a few seconds, a message appears reminding you of other tasks to perform if you are deleting a role.
  4. Read the reminder, then click **OK**.
  5. Click **OK** to clear the confirmation message.
  6. Click **Enforce** on the toolbar, review the effects of enforcing in the [Enforce Preview window](#) (if it is enabled), then click **Enforce** on that window.
  7. Make sure you do the following, if they apply:
    - Change the default role on any ports that may be using the role. You can use the [Port Properties window General tab](#) for the port to do this, or, if there are multiple ports to be changed, use the [Port Configuration Wizard](#).
    - Re-enable authentication on any ports that were disabled before you deleted the role. You can use the [Port Properties window Authentication Configuration tab](#) for the port to do this, or, if there are multiple ports to be reset, use the [Port Configuration Wizard](#).
- 

## Related Information

For information on related concepts:

- [Authentication](#)
- [Traffic Classification Rules](#)

For information on related tasks:

- [Assigning Default Roles to Ports](#)
- [Clearing Default Roles from Ports](#)
- [Creating a Service Using the Service Wizard](#)
- [How to Make Selections on Add/Remove Windows](#)
- [Setting Port Authentication](#)
- [Using the Port Configuration Wizard](#)

For information on related windows:

- [Add/Remove Services Window](#)
- [General Tab \(Role\)](#)
- [Ports Tab \(Role\)](#)
- [Port Properties - General Tab](#)

## How to Create a Service

---

Services are sets of [rules](#) that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. Policy Manager allows you to create Local Services (services that are unique to the current domain) and Global Services (services that are common to all domains). Global Services let you easily create and manage services that are shared between all your domains.

Services can be one of two types: Manual Service or Automated Service.

- **Manual Service** 🍀 - This service consists of one or more [traffic classification rules](#) that you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- **Automated Service** 🍀 - This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group or groups. You create a network resource group using a list of MAC or IP addresses, and then associate the group with the Automated service (see [How to Create a Network Resource](#) for more information). Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

There are two ways to create a service:

- **Using the Service Wizard:** The Service Wizard is a series of windows that leads you through all the steps required to create either type of service, including defining the traffic classification rules that will apply to a Manual service. The first two Service Wizard windows ask you to provide a name for the service and specify whether it is a Manual or Automated service. The subsequent windows depend on whether or not the service is Manual or Automated. If it is Manual, they are similar to the [Rule Wizard](#) windows, except that you can create as many rules as you need without leaving the wizard. Use the Service Wizard if you want to create all the rules for a service at once.
- **Using the Service Tabs:** Creating a service using the service tabs consists of creating a name for the service using the **Create Service** menu option, and defining the service using the service General tab. If you are creating a

Manual service, you can then use the [Classification Rule Wizard](#) (or the Create Rule menu option and the tabs for the rule) to define the rules for the service. Creating a service this way accomplishes the same things as the Service Wizard, but enables you to do only those parts of the procedure you want to do, when you want to do them. You can also use the service tabs and rule tabs to modify an existing service and its rules.

Once you've created a service, you can apply it to any number of [roles](#) in Policy Manager. A role may utilize both Manual and Automated services.

Instructions on:

- [Using the Service Wizard](#)
- [Using the Service Tabs](#)
- [Modifying a Service](#)
- [Saving Services to a .pmd File](#)
- [Deleting a Service](#)

## Using the Service Wizard

The Service Wizard is a series of windows that leads you through all the steps required to create a service. During the creation of a service, you will be asked to decide whether the service is [Manual](#) or [Automated](#).

---

**NOTE:** The Service Wizard is accessed from the Role Wizard if you elect to create a new service while creating the role. The Service Wizard opens, then returns you to the Role Wizard after the service has been created. If you have accessed the Service Wizard from the Role Wizard, you can skip the first two steps of the procedure below.

---

1. In the Policy Manager left panel, select the Services tab.
2. Expand either the Local Services folder or the Global Services folder depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the Services folder and select Service Wizard.
4. In the **Service Name window**, type a name for the service. (The service name is case-sensitive; therefore, Policy Manager sees "Engineer" and "engineer" as two different service names.) Click **Next**.
5. In the **Service Type window**, select either [Manual](#) or [Automated](#), and click **Next**. The subsequent windows depend on which type of service you are

creating.

**For a Manual service:**

- a. In the **Rule Name window**, type a name for the first rule you want to apply to this service, and click **Next**. You will now be creating the rule. For more information on what you will encounter in the following windows, see [Traffic Classification Rules](#) and/or [How to Create or Modify a Rule](#).
- b. In the **Rule Status window**, you can elect to disable the rule at this time. If you disable the rule, it is temporarily unavailable for use by the current service, but it can still be copied to other services and enabled, or re-enabled at another time for the current service. Click **Next** to continue.
- c. In the **Rule Type window**, specify the type of device the rule will apply to when enforced. The recommended selection is All Devices, unless there is a specific need for a device-specific rule, such as when support for a traffic description and/or action is not available on all managed devices. In that case, you can create a rule specific to a certain device type.
- d. In the **Rule TCI Overwrite window**, specify the TCI Overwrite functionality for the rule:
  - **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
  - **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
  - **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.
- e. In the **Traffic Classification Layer window**, select All Layers or a specific Traffic Classification Layer and click **Next**. Each layer has multiple Classification Types. See [Classification Types and their Parameters](#) for a description of classification layers and types.

- f. Select the desired Classification Type and click **Next**.
- g. Each Classification Type requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information. Select and/or enter the required parameters and click **Next**.
- h. In the **Actions window**, define the actions to apply to the rule, then click **Next** to continue. Actions apply access control, class of service, and/or accounting and security behavior to packets matching the rule.
  - **Access Control:** Choose one of the following options:
    - **None** - No default access control specified.
    - **Permit Traffic:** Allows traffic to be forwarded with the port's assigned VID.
    - **Deny Traffic:** Traffic will be automatically discarded.
    - **Contain to VLAN:** If you want to contain traffic for this rule, select this option, then select the appropriate VLAN from the list.
  - **Class of Service:** Use the drop-down list to select a class of service for the traffic.
  - **Accounting/Security:** When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use these options to specify certain rule usage actions to take place when a "rule hit" is reported. Specifying "Prohibited" will prevent lower priority rules and the role's default actions from triggering the action.
    - **System Log:**
      - **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
      - **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.


- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.
- **Audit Trap:**
  - **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
  - **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.
- **Disable Port:**
  - **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
  - **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.
- **Quarantine Role:**
  - **Select Role** - Use the drop-down list to select the role that you want to assign as a [Quarantine role](#).
  - **Disabled** - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-

precedence rules may still specify a Quarantine role for this data packet if there is a match.

- **Prohibited** - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.

- **Traffic Mirror:**

- **Select port group(s)** - Use the drop-down list to specify the port groups where [mirrored traffic](#) will be sent for monitoring and analysis.

You will see an option below to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to a Application Analytics appliance. The Application Analytics appliance only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and appliance. By default this number is set to 10, but can be changed by clicking on the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.

- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

i. In the **Classification Rule Summary window**, view the rule(s) for the service.

- To remove a rule from the service, select it, then click **Remove**.
- To add another rule to the service, click **Add**. This returns you to the rule Name window. Repeat steps a through h.

**Note:** When you add more than one rule to a service, Policy Manager checks for conflicts with other rules in the service. See [Conflict Checking](#) for more information.



- j. In the **Service Role window**, you can select the role(s) to which the service will apply. If you want to create a new role to add to the list before selecting, click **New**.
- k. Click **Finish** and the service will be created under the Manual Services folder in the left-panel tree. Go on to [step 6](#).  
**Note:** If you came to the Service Wizard via the Role Wizard, you will return to the Role Wizard when you click **Finish**.

#### For an Automated service:

- a. In the **Rule TCI Overwrite window**, specify the TCI Overwrite functionality for the rule:
  - **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
  - **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
  - **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.
- b. In the **Automated Rules window**, select the network resource type (Layer 2 MAC or Layer 3 IP). This will determine the list of network resources available for selection for this service. Select the type of rule you want to create. Some rule types require that you enter certain parameters and/or values; see [Classification Types and their Parameters](#) for parameter information. Select the network resources to which the service will apply by clicking the **Add** button.
- c. In the **Actions window**, define the actions to apply to the rule, then click **Next** to continue. Actions apply access control, class of service, and/or accounting and security behavior to packets matching the rule.

- **Access Control:** Choose one of the following options:
  - **None** - No default access control specified.
  - **Permit Traffic:** Allows traffic to be forwarded with the port's assigned VID.
  - **Deny Traffic:** Traffic will be automatically discarded.
  - **Contain to VLAN:** Contains traffic to a specific VLAN. Select the appropriate VLAN from the list. If you want to [create a new VLAN](#) to add to the list, click the menu button to the right of the VLAN field and click **Add**.
- **Class of Service:** Select the desired class of service in the list. To create a new Class of Service to add to the list, click the menu button to the right of the field and click **Add**. The Create Class of Service window opens where you create a new Class of Service.
- **Accounting/Security:** When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use these options to specify certain rule usage actions to take place when a "rule hit" is reported. Specifying "Prohibited" will prevent lower priority rules and the role's default actions from triggering the action.
  - **System Log:**
    - **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
    - **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
    - **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.
  - **Audit Trap:**
    - **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.

- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.
- **Disable Port:**
  - **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
  - **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.
- **Traffic Mirror:**
  - **Select port group(s)** - specify port groups where [mirrored traffic](#) will be sent for monitoring and analysis.
  - **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

- d. In the **Service Role window**, you can select the roles to which the service will apply. If you want to create a new role to add to the list before selecting, click **New**.
  - e. Click **Finish** and the service will be created under the Automated Services folder in the left-panel tree. Go on to [step 6](#).  
**Note:** If you came to the Service Wizard via the Role Wizard, you will return to the Role Wizard when you click **Finish**.
6. To add a detailed description for the service, select the service in the left panel and the General tab in the right panel. Click the **Edit** button to enter a description in the **Description** field.
  7. Now that the service has been created, you can:
    - [Add the service to a role](#)
    - [Add the service to a service group](#)
  8. [Enforce](#) to write the new information to the devices.

## Using the Service Tabs

The following steps depend on whether you are creating a [Manual](#) or an [Automated](#) service. For an Automated service, you will create the service and use the General tab to define the class of service and/or access control for the service. For a Manual service, you will create the service and then use the [Classification Rule Wizard](#) (or the Create Rule menu option and the tabs for the rule) to define the rules for the service.

### *Creating an Automated Service*

1. In the left panel, select the Services tab.
2. Expand either the Local Services folder or the Global Services folder depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the Services folder and select Create Automated Service. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the highlighted box. The service name is case-sensitive; therefore, Policy Manager sees "Engineer" and "engineer" as two different service names. Press the **Enter** key. If you don't do this, the name will remain "New Service."

5. In the service General tab, define the rule's traffic description and actions, and enter a description of the service, if desired. For information on configuring the fields on this tab, see the [General Tab \(Service\)](#) Help topic.
6. [Enforce](#) to write the new information to your devices.

### *Creating a Manual Service*

1. In the left panel, select the Services tab.
2. Expand either the Local Services folder or the Global Services folder depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the Services folder and select Create Service. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the highlighted box. The service name is case-sensitive; therefore, Policy Manager sees "Engineer" and "engineer" as two different service names. Press the **Enter** key. If you don't do this, the name will remain "New Service."
5. In the service [General tab](#), enter a description for the service, if desired.
6. Define rules for the service, as follows:
  - *To associate an existing rule with the new service:* In the left panel Services tab, open a service you know has the rule, then drag the rule to the new service. This creates a copy of the existing rule, with all its characteristics. To give the rule another name, right-click the copy, select **Rename**, then type the new name in the highlighted box.
  - *To create new rules for the service:* Use one of the following methods:
    - [Using the Classification Rule Wizard](#)
    - [Using the Rule General Tab](#)

**Note:** When you add more than one rule to a service, Policy Manager checks for conflicts with other rules in the service. See [Conflict Checking](#) for more information.

7. [Enforce](#) to write the new information to your devices.

## Modifying a Service

Once you've created a service, you can change its characteristics by selecting the service or its rules in the left-panel Services tab and using the menu options or associated right-panel tabs.

- [Modifying a Service Description](#)
- [Modifying a Service Name](#)
- [Modifying the Roles for a Service](#)
- [Modifying the Rules for a Manual Service](#)
- [Modifying an Automated Service](#)

### *Modifying a Service Description*

You can edit the description for the service on the service [General tab](#). Click **Save** to save the change to the database.

### *Modifying a Service Name*

1. In the left panel, select the Services tab.
2. Expand the Local or Global Services folder and then the Services folder, and select the service you want to modify.  
**Note:** If the service is a member of a service group and it's more convenient, you can find the service under the service group in the Service Groups folder. Any change you make to the name there will also be reflected in the Services folder.
3. Right-click the service whose name you want to change, and select **Rename**.
4. Type the new name in the highlighted box.
5. Click **Save** to save the change to the database.

### *Modifying the Roles for a Service*

You can see all the roles associated with a particular service in the Role/Service Usage window.

1. In the left-panel Services tab, select the service you want to modify.

2. Right-click on the service and select **Role Usage** from the menu. The Role/Service Usage window opens where you can view and edit the roles associated with the service.

To modify the roles associated with a service, use the role [Add/Remove Services window](#), which you can access from the Role/Service Usage window as follows:

1. Select a role, then click **View/Edit Role**. This opens the left-panel Roles tab with the role selected, and the [General tab](#) in the right panel.
2. In the Services section, click the **Add/Remove Services** button. This opens the role [Add/Remove Services window](#), where you can:
  - [Add](#) the service or any other service to any role.
  - [Remove](#) the service from the selected role or from any other role.
3. [Enforce](#) to write the new information to your devices.

### *Modifying the Rules for a Manual Service*

1. Select the left-panel Services tab and locate the service you want to modify in the Manual Services folder.  
**Note:** If the service is a member of a service group and it's more convenient, you can find the service under the service group in the Service Groups folder. Any change you make to the rule there will also be reflected in the Manual Services folder.
2. Expand the service so that its rules are displayed.
3. Select the rule you want to change, then use the right-panel tabs to make your changes.
4. [Enforce](#) to write the new information to your devices.

### *Modifying an Automated Service*

1. Select the left-panel Services tab and locate the service you want to modify in the Automated Services folder.  
**Note:** If the service is a member of a service group and it's more convenient, you can find the service under the service group in the Service Groups folder. Any change you make to the service there will also be reflected in the Automated Services folder.
2. Select the [General tab](#) in the right panel

3. To change the Network Resources with which the service is associated, use the Network Resources drop-down list to select a new network resource group.
4. Modify the remaining characteristics of the Automated service as required. For information on configuring the fields on this tab, see the [General Tab \(Service\)](#) Help topic.
5. [Enforce](#) to write the new information to your devices.

## Saving Services to a .pmd File

Policy Manager enables you to save a service or services to a Policy Manager database (.pmd) file, allowing you to import the services into another domain. When you create a file name, keep the following in mind:

- Special characters such as `/\ : ? " < > |` are not allowed.
- On the Windows platform, the file name is not case-sensitive; therefore, Policy Manager sees X.pmd and x.pmd as the same file name.
- On the Linux platform, the file name is case-sensitive; therefore, Policy Manager sees X.pmd and x.pmd as two different file names.

### To save a single service:

1. Select the left-panel Services tab.
2. Expand the Services folder.
3. Right-click the service in the left panel and select **Export Service(s) To File**.
4. In the File name field, enter a name for the .pmd file.
5. Click **Save**, then click **OK** to clear the confirmation message.

### To save multiple services:

1. Select the left-panel Services tab.
2. Select the Services folder (or select the Service Groups folder and then a service group).
3. In the right Details View panel, hold down the **Shift** key (for sequential services) or **Ctrl** key (for non-sequential services) key and select the services.
4. Right-click the services and select **Export Service(s) To File**.



5. In the File name field, enter a name for the .pmd file.
6. Click **Save**, then click **OK** to clear the confirmation message.

## Deleting a Service

Deleting a service removes the service and its rules. If copies of the rules exist for other services, those copies are not affected by the deletion. However, deleting the service removes it from any service groups and roles with which it was associated, so be sure the service is not needed before you delete it. Deleting a Global service deletes the service from all your domains.

1. Select the left-panel Services tab.
2. Expand the Services folder.  
**Note:** If the service is a member of a service group and it's more convenient, you can alternatively find the service under the service group in the Service Groups folder. Deleting the service there also deletes the service wherever else it exists.
3. Right-click the service you want to delete, and select **Delete**.
4. Click **Yes** to confirm, then **OK** to clear the confirmation message.
5. [Enforce](#) to write the change to your devices.

---

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [Adding Services to Roles](#)
- [Adding Services to Service Groups](#)
- [Creating Service Groups](#)
- [How to Create a Class of Service](#)
- [How to Create a Network Resource Group](#)
- [How to Create or Modify a Rule](#)
- [How to Define a Rate Limit](#)
- [Using the Rule Wizard](#)
- [Using the Traffic Description Wizard](#)

For information on related windows:

- [Details View Tabs](#)
- [General Tab \(Service\)](#)

## How to Create a Service Group

---

Policy Manager lets you create service groups into which you can group Local and Global [services](#). A service group can contain any number of services, as well as other service groups. A service can be a part of more than one group.

Instructions on:

- [Creating a Service Group](#)
- [Adding Services to a Service Group](#)
- [Removing Services from a Service Group](#)

### Creating a Service Group

1. Select the left-panel Services tab. Expand the Local Services or Global Services folder.
2. Right-click on the Service Groups folder and select Create Service Group. This expands the Service Groups folder and creates a "New Service Group" item.
3. Type the service group name in the highlighted box and press **Enter**. You can now [add services](#) to the service group. Once a service group has been created at the top level under the Service Groups folder, it can be added to another service group.

### Adding Services to a Service Group

A service group can contain any number of services, as well as other service groups. You can add services to a service group using the following methods:

- *Dragging and dropping services:* You can drag and drop a single service from the left panel to the service group, or drag and drop multiple services from the right-panel Details View.
- *Dragging and dropping service groups:* You can drag and drop a single service group from the left panel to the service group, or drag and drop multiple service groups from the right-panel Details View.
- *Using the Add/Remove Services/Service Groups menu option:* Right-click the service group and select Add/Remove Services/Service Groups. In the

Add/Remove Services window, select the services or service groups you want to add, and click **Add**. Click **OK**.

## Removing Services from a Service Group

Use the following steps to remove a service or service group from a service group. Removing a service from a service group does not delete the service itself. If you want to delete the service itself, see [Deleting a Service](#). Keep in mind that if you change the contents of a service group, Policy Manager automatically updates the services list for any role that the service group is associated with, affecting the rules that are in the role.

1. Right-click the service group from which you wish to remove services, and select Add/Remove Services.
2. In the Add/Remove Services window, select the services or service groups you want to remove from the service group, and click **Remove**.
3. Click **OK**.

Alternatively, you can right-click a service or service group and select **Remove Service(s) from Group** or **Remove Service Group(s) from Group** from the menu.

---

### Related Information

For information on related tasks:

- [How to Create a Service](#)
- [Deleting a Service](#)

For information on related windows:

- [Add/Remove Services \(Roles\) Window](#)

## How to Create a VLAN

---

Policy Manager VLANs which can be used for access control are displayed in the Access Control Configuration window (available from the Policy Manager Edit menu). If you have enabled the [Policy VLAN Islands](#) feature, there are two VLANs folders in this window: [Global VLANs](#) and [Policy VLAN Islands](#) . Otherwise, only the Global VLANs folder is displayed. For more information on Policy VLAN Islands, see [How to Create a Policy VLAN Island](#).

Policy Manager provides you with one Global Default VLAN, which is available when you first start using Policy Manager. You can create additional VLANs using the Create VLAN option available when you right-click on the Global VLANs folder.

Once a VLAN is created, you can use it as follows:

- as the default access control for a role, using the role [General Tab](#) or [Role Wizard](#)
- as an access control action for a rule using the rule [General tab](#) or [Rule Wizard](#)
- as an access control action for an automated service, using the service [General Tab](#) or [Service Wizard](#)
- in a Policy VLAN Island, if that feature is enabled

You can view the roles and services associated with a VLAN by right-clicking on the VLAN in the left panel and selecting Role/Service Usage. You can also make role and service changes from the Role/Service Usage window.

See [Create VLAN Window](#) and [Roles](#) for additional information.

Instructions on:

- [Creating a VLAN](#)
- [Editing an Island VLAN ID](#)
- [Deleting a VLAN](#)
- [Turning Off Getting VLANs on Startup](#)

## Creating a VLAN

1. Open the Access Control Configuration window (available from the Policy Manager Edit menu).
2. Right click the Global VLANs folder and select **Create VLAN** from the menu.
3. Fill out the [Create VLAN Window](#) to your specifications.
4. To create the VLAN and close the Create VLAN window, click **OK**. To create a VLAN and leave the window open, click **Apply**.
5. [Enforce](#) to write the new information to the devices.

## Editing an Island VLAN ID

1. Open the Access Control Configuration window (available from the Policy Manager Edit menu).
2. Expand the Policy VLAN Islands folder, and select the Policy VLAN Island with which the island VLAN is associated.
3. Select the VLANs tab in the right panel.
4. Select the Island VLAN and click **Edit Island VLAN ID**.
5. Enter the new VLAN ID and click **OK**.
6. [Enforce](#) to write the new information to the devices.

## Deleting a VLAN

Deleting a VLAN removes it and its associations with any roles and services from the Policy Manager database and from the devices.

---

**WARNING:** The delete operation will immediately remove the VLAN(s) from the devices in the Network Elements tab and could result in serious consequences if the VLANs are used outside the scope of Policy Manager.

---

1. Open the Access Control Configuration window (available from the Policy Manager Edit menu).
2. Right click on the VLAN you wish to delete and select **Delete** from the menu. A confirmation window opens.

3. Click **Yes** to delete the VLAN.
4. [Enforce](#) to write the new information to the devices.

## Turning Off Getting VLANs on Startup

When Policy Manager is launched, it automatically reads the VLANs from the devices. However, this can take some time when you have many VLANs and devices. If it is not required that Policy Manager and the devices be synchronized each time you launch Policy Manager, you can turn off the reading of VLANs at launch by deselecting the Get VLANs on Startup option in the Options [Startup view](#) (Tools > Options).

---

### Related Information

For information on related concepts:

- [Dynamic Egress](#)
- [Policy VLAN Islands](#)

For information on related windows:

- [Create VLAN Window](#)
- [General Tab \(Role\)](#)
- [Startup View Options Window](#)

## How to Create a Policy VLAN Island

---

VLAN islands enable you to set up, for example, a guest VLAN that restricts the guests in one facility from communicating with guests in another facility. See [Policy VLAN Islands](#) for more information.

Instructions on:

- [Creating a VLAN Island](#)
- [Modifying a VLAN Island](#)
- [Deleting a VLAN Island](#)

### Creating a VLAN Island

You can create a Policy VLAN Island as follows:

**Note:** VLANs used in VLAN islands must be Island VLANs.

1. Open the Access Control Configuration window (available from the Policy Manager Edit menu).
2. In the left-panel of the Access Control Configuration window, click Policy VLAN Islands.
3. In the right-panel, click the [VLANs Tab](#) and click **Create**.
4. In the **Create VLAN** window, enter a name for the VLAN. Click **OK**.
5. Click **Close**.

### Modifying a VLAN Island

Once you've created a VLAN island, you can change its characteristics using the right-panel tabs as follows:

- *To change a VLAN island name:* Right-click the island in the left-panel of the VLANs window and select **Rename**.
- *To change a VLAN island description:* Use the island's [Island Topology tab](#).
- *To edit an Island VLAN ID:* Use the **Edit Island VLAN ID** button on the island's [VLANs tab](#).



- *To change a VLAN Island Configuration (Base ID, Offset, Naming Convention):* Use the Policy VLAN Islands folder [Island Topology tab](#) .
- *To add or remove devices from a VLAN island:* Use the VLAN Islands [Add/Remove Devices window](#).

## Deleting a VLAN Island

You cannot delete the Default Island.

1. Open the Access Control Configuration window and expand the Policy VLAN Islands folder.
2. In the left-panel of the Access Control Configuration window, expand Policy VLAN Islands.
3. Right-click the island you want to delete and select **Delete**.
4. Click **Yes** to confirm the deletion.

---

### Related Information

For information on related concepts:

- [Policy VLAN Islands](#)

For information on related windows:

- [Add/Remove Devices window](#)
- [VLANs Tab \(Policy VLAN Islands\)](#)
- [Island Topology Tab \(Policy VLAN Islands\)](#)

## How to Create and Use Domains

---

Policy Manager provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. For example, a university may have a Dormitory domain with a policy configuration created for students, and an Administration domain with a policy configuration for staff members.

You can create multiple domains and easily switch from one domain to another. You can also export policy domain configuration data to a .pmd file, (one file per domain) for backup and troubleshooting purposes, and you can import data from a .pmd file into a policy domain.

In order for your network devices to be displayed in the Policy Manager Network Elements tree, they must be assigned to a Policy Domain. Initially, you must use Console to add your devices to the NetSight database. Once your devices are in the database, you can assign the devices to a Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy Manager Network Elements tree. Only devices that support policy are displayed in the Policy Manager tree.

Policy Manager automatically locks the current Policy Domain when you begin to edit the domain configuration. Other Policy Manager clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released. For more information, see [Controlling Client Interactions with Locks](#). After a modification is made, you must save the domain to notify all clients that are viewing that domain of the change, and automatically update their view with the new configuration.

Instructions on:

- [Creating a New Domain](#)
- [Opening a Domain](#)
- [Assigning Devices to a Domain](#)
- [Removing Devices From a Domain](#)
- [Importing a File into a Domain](#)
- [Exporting a Domain to a File](#)
- [Generating a Policy Report for a Domain](#)

- [Importing Data from a Domain](#)
- [Saving a Domain](#)
- [Reading a Domain](#)
- [Renaming a Domain](#)
- [Deleting a Domain](#)

## Creating a New Domain

Use these steps to create a new Policy Domain.

1. Select **Domain > Create**.
2. Enter the name for the new domain. Select the **Do Not Use Global Services** checkbox if you don't want the domain to include and display services that are common to all domains. Click **OK**.
3. A new (blank) Policy Manager Domain opens.
4. Proceed with [assigning devices](#) to the domain and then configuring the desired policies.

## Opening a Domain

In Policy Manager, you work in one current domain at a time. To change to a different domain, use the Domain menu to select the desired domain. If you have made changes to the current domain, you will be prompted to update the database with the current domain configuration prior to opening the new domain.

## Assigning Devices to a Domain

Initially, you must use Console to [add your devices](#) to the NetSight database. Once your devices have been added to the database, you must assign the devices to a Policy Domain. A device can exist in only one Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy Manager Network Elements tree. Only devices that are assigned to the Policy Domain you are currently viewing are displayed in the tree.

Use these steps to assign devices to a Policy Domain.

1. If necessary, [open the domain](#) that you want to assign devices to.
2. Select **Domain > Assign Devices to Domain**. The [Assign Devices to Domain window](#) opens.
3. Devices that are in the database but not assigned to a domain are listed in the left-panel Unassigned folder (including devices that do not support policy). The left panel also displays any other domains and the devices assigned to those domains. Use the drop-down list to select a single domain or All Other Domains. If you select All Other Domains, use the bottom panel to view which domain each device is assigned to.
4. The right panel displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and click **Add**. You can also select and add multiple devices.
5. To remove a device from the current domain, select the device and click **Remove**. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from. It does not delete the device from the NetSight database.
6. Click **OK**.
7. The selected devices are assigned to the current domain and displayed in the Policy Manager Network Elements tree. (Only devices that support policy are assigned to the domain and displayed in the Policy Manager tree.)

## Removing Devices From a Domain

Removing a device from a domain, removes the device from the Policy Manager Network Elements tree and places it in the Unassigned folder in the Assign Devices to Domain window.

**NOTE:** Removing a device from a domain does not delete the device from the NetSight database. To [delete a device from the database](#), right-click on the device in the left-panel Network Elements tab, and select **Delete** from the menu. When a device is deleted from the database, it is automatically removed from the Console and Policy Manager device tree.

1. If necessary, [open the domain](#) that you want to remove devices from.
2. Select **Domain > Assign Devices to Domain**. The [Assign Devices to Domain window](#) opens.
3. The right panel displays the current domain and the devices assigned to that domain. To remove a device from the current domain, select the device

and click **Remove**. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from. It does not delete the device from the NetSight database.

4. Click **OK**.

## Importing a File into a Domain

You can import policy data from a .pmd file into a Policy Domain.

1. Make sure that the domain you want to import a file into is your current domain.
2. Select **File > Import > Import From File**. The [Import from File window](#) opens.
3. Enter the name and path for the data file (.pmd) you want to import, or browse to the file. If you click **Browse**, you will see multiple .pmd files to select from. These different PMDs are designed for typical networking requirements. They contain Policy Manager roles and rules appropriate for the specific scenario.
4. Select the specific data elements you want to import or click **Select All** to select all the data import options at once. See [Data Elements to Import](#) for important information on each element and how they will be imported.
5. Select how you want the imported data applied to your current domain. Click on the links below for detailed information on how each specific action affects the import of certain data elements.
  - [Append](#) data to existing elements
  - [Update](#) existing data with elements from domain
  - [Overwrite](#) existing elements
6. Click **OK**. The data elements will be imported and you will see a message regarding import status.

**NOTE:** If you decide that you want to return to the previous configuration (that the import overwrote), you can perform a **File > Read Policy Domain** operation to restore the configuration, as long as you have not saved the data you imported.

## Exporting a Domain to a File

You can export policy data from a Policy Domain to a .pmd file.

1. If necessary, [open the domain](#) that you want to export to a file.
2. Select **File > Export to File**.
3. Navigate to the directory where you want to save the .pmd file.
4. In the **File name** field, enter the name of the file with the .pmd extension. Special characters such as `/\ : ? " < > |` are not allowed in the file name. On the Windows platform, the file name is not case-sensitive; therefore, Policy Manager sees X.pmd and x.pmd as the same file name. On the Linux platform, the file name is case-sensitive; therefore, Policy Manager sees X.pmd and x.pmd as two different file names.
5. From the Files of type drop-down list, select Policy Manager Database files (\*.pmd).
6. Click **Save**.

## Generating a Policy Report for a Domain

You can generate a summary report of the current domain's policy configuration in PDF format. Each report contains a description of the domain, plus a detailed summary of each of the domain's roles and services, and the rules contained in each service. In addition, the report provides information on the devices assigned to the domain, the domain's Network Resources, Class of Service information (including transmit queues and rate limiting information), and VLAN information.

1. Make sure that the domain you want to generate a report on is selected as your current domain.
2. Select **Domain > Generate Policy Report**.
3. The report is saved to the following directory: `Documents and Settings\\Application Data\NetSight\System\PolicyMgr`.

## Importing Data from a Domain


You can import policy configuration data from one policy domain into another.

1. Make sure that the domain you want to import data into is your current domain.

2. Select **File > Import > Import From Domain**. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.) The [Import from Domain window](#) opens.
3. Use the drop-down list to select the domain whose data you want to import.
4. Select the specific data elements you want to import or click **Select All** to select all the data import options at once. See [Data Elements to Import](#) for important information on each element and how they will be imported.
5. Select how you want the imported data applied to your current domain. Click on the links below for detailed information on how each specific action affects the import of certain data elements.
  - [Append](#) data to existing elements
  - [Update](#) existing data with elements from domain
  - [Overwrite](#) existing elements
6. Click **OK**. The data elements will be imported and you will see a message regarding import status.

**NOTE:** If you decide that you want to return to the previous configuration (that the import overwrote), you can perform a **File > Read Policy Domain** operation to restore the configuration, as long as you have not saved the data you imported.

## Saving a Domain

After a Policy Domain has been changed, you must save the domain to notify all clients that are viewing that domain of the change and automatically update their view with the new configuration. A Save icon  is displayed in the status bar when you have made changes to the domain that need to be saved. You can save a Policy Domain by selecting **File > Save Policy Domain** or by clicking the Save toolbar button.

## Reading a Domain

Reading a Policy Domain lets you update your current Policy Domain with the latest saved domain data. You can read a Policy Domain by selecting **File > Read Policy Domain** or by clicking the Read toolbar button.

## Renaming a Domain

You can rename the current Policy Domain by selecting **Domain > Rename** and entering a new name.

## Deleting a Domain

You can delete one or more Policy Domains by selecting **Domain > Delete**.

---

### Related Information

For information on related tasks:

- [How to Add and Delete Devices](#)

For information on related windows:

- [Assign Devices to Domain Window](#)
- [Import from Domain Window](#)
- [Import from File Window](#)



## How to Create or Modify a Rule

---

Traffic Classification rules allow you to assign a class of service and/or access control (VLAN membership) to network traffic, depending on the traffic's classification type. Classification types are based on layers 2, 3, and 4 of the OSI model, and traffic is classified according to specific layer 2/3/4 information contained in each frame. For more information, see [Traffic Classification Rules](#).

A rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the type of traffic to which the rule will pertain. Actions specify whether that traffic will be assigned class of service, access control, or both.

There are two ways to create a rule:

- **Using the Classification Rule Wizard:** The Classification Rule Wizard is a series of windows that leads you through all the steps required to create a rule, including defining the traffic description and the actions that will apply to it.
- **Using the Rule Tabs:** Creating a rule manually consists of creating a name for the rule using the **Create Classification Rule** menu option, then using the rule's right panel General tab to specify its characteristics. Creating a rule using this method accomplishes the same things as the Classification Rule Wizard, but enables you to do only those parts of the procedure you want to do, when you want to do them. You can also use the right-panel General tab to modify an existing rule.

In order to create a rule, you must first [create a service](#) with which to associate it.

Instructions on:

- [Using the Classification Rule Wizard](#)
- [Using the Rule General Tab](#)
- [Disabling/Enabling a Rule](#)
- [Deleting a Rule](#)


## Using the Classification Rule Wizard

The Classification Rule Wizard is a series of windows that lead you through all the steps required to create a new rule.

1. In the Policy Manager left panel, select the Services tab.
2. Expand either the Service Groups or Services folder and select the service for which you want to create a rule.
3. From the menu bar, select **Tools > Classification Rule Wizard**. You can also right-click on the service and select the option from the menu. The Rule Wizard opens.
4. In the **Name window**, enter a name for the rule and click **Next**.
5. In the **Rule Status window**, you can elect to disable the rule at this time. If you disable the rule, it is temporarily unavailable for use by the current service, but it can be re-enabled at any time or copied to other services and enabled. See [Disabling a Rule](#) for more information. Click **Next** to continue.
6. In the **Rule Type window**, specify the type of devices to which you wish this rule to apply when enforced. See [Rule Type](#) for more information on the consequences of your choice. Click **Next** to continue.
7. In the **Rule TCI Overwrite window**, specify the TCI Overwrite functionality for the rule:
  - **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
  - **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
  - **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.
8. In the **Traffic Classification Layer window**, select All Layers or a specific Traffic Classification Layer and click **Next**. Each layer has multiple Classification Types. See [Classification Types and their Parameters](#) for a description of classification layers and types.
9. In the **Traffic Types window** for your previous selection, choose the desired Classification Type and click **Next**.

10. Each Traffic Classification Type requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information. Select and/or enter the required parameters and click **Next**.
11. In the **Actions window**, define the actions to apply to the rule, then click **Next** to continue. Actions apply class of service, access control, and/or accounting and security behavior to packets matching the rule.
  - **Access Control:** To assign access control (a VLAN), use the drop-down list to select one of the following options:
    - **Permit Traffic:** If you want to allow traffic to be forwarded with the port's assigned VID, select this option.
    - **Deny Traffic:** traffic will be automatically discarded.
    - **Contain to VLAN:** If you want to contain traffic for this rule, select this option, then select the appropriate VLAN from the list.
  - **Class of Service:** To assign a class of service to the traffic, use the drop-down list to select a class of service for the traffic.
  - **Accounting/Security:** When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use these options to specify certain rule usage actions to take place when a "rule hit" is reported. Specifying "Prohibited" will prevent lower priority rules and the role's default actions from triggering the action.
    - **System Log:**
      - **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
      - **Disabled** - If this option is disabled and this rule is hit, it does not generate a syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
      - **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.
    - **Audit Trap:**
      - **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.

- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.
- **Disable Port:**
  - **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
  - **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.
- **Quarantine Role:**
  - **Select Role** - Use the drop-down list to select the role that you want to assign as a [Quarantine role](#).
  - **Disabled** - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.
- **Traffic Mirror:**
  - **Select port group(s)** - Use the drop-down list to specify the port groups where [mirrored traffic](#) will be sent for monitoring and analysis.  
You will see an option below to mirror only the first (N)

packets of a flow. This option is intended for use when mirroring traffic to a Application Analytics appliance. The Application Analytics appliance only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and appliance. By default this number is set to 10, but can be changed by clicking on the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.

- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

12. Click **Finish**.

13. [Enforce](#) to write the new information to the devices.

## Using the Rule General Tab

When you create a rule using the rule [General tab](#), you first create and name the rule using the **Create Classification Rule** menu option, then define its characteristics in the General tab. You can also use the General tab to modify an exiting rule's characteristics.

1. In the Policy Manager left panel, select the Services tab.
2. Expand either the Service Groups or Services folder and click on the service for which you want to create a rule.
3. Right-click on the service and select **Create Classification Rule**.
4. In the [Create Classification Rule window](#), enter a name for the rule, and select the rule status and type. Click **OK**. The rule is created in the left-panel tree. You can now use the associated right-panel General tab to define the rule. Refer to the [General tab](#) Help topic for information on configuring the rule.
5. [Enforce](#) to write the new information to the devices.

## Disabling/Enabling a Rule

In Policy Manager, you can disable and enable individual or multiple rules. You can also disable and enable all the rules associated with a service, or all the rules for all the services in a service group. The rule icon in the left panel displays a red X if the rule is disabled.

Disabling a rule is an alternative to deleting and recreating it. If you disable a rule, it is temporarily unavailable for use by the service with which it is associated. However, the rule can be copied to another service and enabled for that service.

### Disabling/Enabling an Individual Rule

These are the instructions for disabling and enabling rules using the rule's [General tab](#). You can also disable/enable rules in the Rule Status window of the [Service Wizard](#) or [Classification Rule Wizard](#), or by right-clicking on the rule and selecting **Disable Rule(s)** or **Enable Rule(s)**.

1. In the Policy Manager left panel, select the Services tab.
2. Expand the Services folder and the service, to locate the rule you want to disable or enable. (If the rule is part of a service that is also a member of a service group, you can expand the Service Groups folder to find the rule.)
3. Select the rule you want to disable or enable, and select the [General tab](#) in the right panel.
4. In the General area, select **Enable** or **Disable** for the Rule Status. Disabling the rule turns on the red X on the rule icon in the left panel, and re-enabling it turns it off.
5. [Enforce](#) to write the new information to the devices.

### Disabling/Enabling Multiple Rules

These are instructions for disabling and enabling multiple rules in a single operation.

1. In the Policy Manager left panel, select the Services tab.
2. Expand the Services or Service Group folder and select the service containing the rules you want to disable or enable.
3. In the right-panel Details View, multi-select the desired rules. Right-click and select **Disable Rule(s)** or **Enable Rule(s)**.
4. [Enforce](#) to write the new information to the devices.

### Disabling/Enabling the Rules for a Service or Service Group

If a service is associated with more than one service group, disabling or enabling

the rules for the service in one service group will disable/enable the rules for the service in the other service groups of which the service is a part.

1. In the Policy Manager left panel, select the Services tab.
2. Expand the Services or Service Group folder.
3. Right-click the service or service group containing the rules you want to disable or enable and select **Disable Rule(s)** or **Enable Rule(s)**.
4. Click **Yes** to confirm the change.
5. [Enforce](#) to write the new information to the devices.

## Deleting a Rule

Deleting a rule removes the rule from a service. If the service is also part of a service group, the rule is deleted there as well, so be sure the rule is not needed before you delete it.

1. In the Policy Manager left panel, click the Services tab.
  2. Expand the Services folder and the service to locate the rule you want to delete. (If the rule is part of a service that is also a member of a service group, you can expand the Service Groups folder to find the rule.)
  3. Right-click the rule you want to delete, and select **Delete**.
  4. Click **Yes** to confirm, then **OK** to clear the confirmation message. The rule is deleted wherever it exists.
  5. [Enforce](#) to write the new information to the devices.
- 

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related windows:

- [Edit Rule Window](#)
- [General Tab \(Rule\)](#)
- [Rule Usage Tab \(Rule\)](#)
- [ToS/DSCP Configuration Window](#)

## How to Define Traffic Descriptions

---

Traffic Classification rules allow you to assign VLAN membership and/or class of service to network traffic based on the traffic's classification type. Traffic descriptions are the part of a rule that defines this classification type. For more information, see [Traffic Classification Rules](#).

The Traffic Description Wizard is used to define traffic descriptions for new rules.

### Accessing the Traffic Description Wizard

Use the following steps to create a new rule, and access the wizard to define the rule's traffic description.

1. In the Policy Manager left panel, select the Services tab.
2. Expand either the Service Groups or Services folder and click on the service for which you want to create a rule.
3. From the menu bar, select **Tools > Create Classification Rule**. You can also right-click on the service and select the option from the menu.
4. In the [Create Classification Rule window](#), enter a name for the rule, and select the rule status and type. Click **OK**. The rule is created in the left-panel tree. You can now use the associated right-panel General tab to define the rule.
5. Click on the rule's [General tab](#). In Traffic Description area, click **Edit** to open the Traffic Description Wizard.

### Using the Traffic Description Wizard

The Traffic Description Wizard is a series of windows that lead you through all the steps required to define a traffic description for a rule.

1. In the Traffic Classification Layer window, select All Layers or a specific Traffic Classification Layer and click **Next**. Each layer has multiple Classification Types. See [Classification Types and their Parameters](#) for a description of classification layers and types.
2. In the Traffic Classification Type window, select the desired Classification Type and click **Next**.



3. Each Classification Type requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information. Select and/or enter the required parameters and click **Finish**.
  4. To apply the rule you have created or modified, click the **Enforce** button on the Policy Manager main tool bar, review the effects of enforcing on the [Enforce Preview window](#) (if it is enabled), then click **Enforce** on that window.
- 

### Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)

For information on related windows:

- [General Tab \(Rule\)](#)

## How to Define Well-Known IDs

---

You can edit the pre-defined list of well-known identifiers (IDs) used when creating Policy Manager rules in the [Pre-Defined Well-Known IDs window](#). You can define a new ID for a TCP/UDP port number (Layer 4 Application Transport traffic classification type) or for an IP Protocol Type (Layer 3 Network traffic classification type). Once defined, these IDs are available for selection from the list of well-known values when defining the rule's traffic classification type.

Use the following instructions to add, remove, or change IDs on the pre-defined list:

1. Select **Edit > Pre-Defined Well-Known IDs** from the menu bar. The **Pre-Defined Well-Known IDs** window opens.
2. Select the **IP Protocol** tab to define an ID that maps to an IP protocol, or select the **Port** tab to define an ID that maps to a TCP/UDP port protocol.

### Adding a new Well-Known ID

- a. Enter the **Port Number** or **IP Protocol** and an associated **Protocol ID**.
- b. Click **Add**. The new ID appears in the table.

### Removing a Well-Known ID

- a. In the table, select the ID(s) that you wish to remove. You can make multiple consecutive selections by holding the left mouse button while swiping the mouse pointer over the table rows or by holding the **Shift** key while clicking. Hold the **Control** key while clicking to make non-consecutive selections.
- b. Click **Remove**. The selected IDs are deleted from the table.

### Changing a Well-Known ID

First remove the ID, then add it with the desired changes.

---

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)

For information on related windows:

- [Pre-Defined Well-Known IDs Window](#)

## How to Enable Passive Domain Mode

---

Setting a Policy Manager domain to passive mode allows you to determine the effectiveness of a policy configuration prior to enforcing the complete domain configuration to your network. This is useful in new Policy Manager deployments, as it provides the ability to test a new policy configuration in a manner that does not disrupt traffic flow in any way, while providing information as to how policy rules are being used. This information can help you determine whether the policy rules you have defined are providing the desired network access.

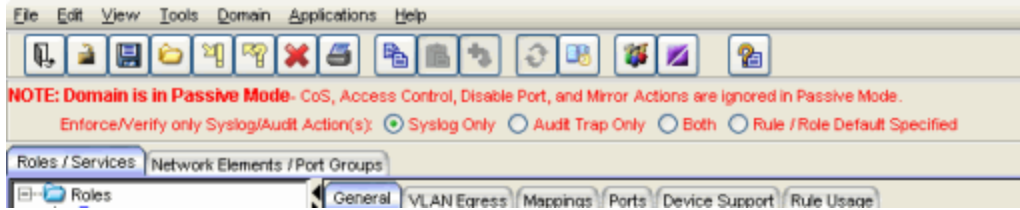
**NOTE:** In order to take advantage of Passive Mode reporting information, devices must support Syslog and Audit Trap actions. Currently, only K-Series, S-Series, and N-Series Platinum devices support this functionality. Enforcing the domain to other devices while in passive mode will result in no rules being written.

While in passive mode, all rule actions which prioritize, contain, or discard traffic (including Class of Service (CoS), Access Control, and Disable Port on Rule Hit as specified on the rule's [General tab](#)), are disabled. A syslog/audit action is specified that provides the capability to collect "rule hit" data. This data shows a traffic description match (rule hit) but does not show what the defined behavior would have been (rate limit/classify/permit/deny/contain) had the domain been enforced in active mode. You will need to configure external tools to make use of the syslog/audit trap data.

**NOTE:** Passive Mode does not disable a role's default actions. Traffic not matching a rule is still dropped if that's the default action for a role.

Following are instructions for enabling passive mode and setting up the syslog/audit action.

1. Select the **Passive Domain Mode** option from the Edit menu in the Policy Manager toolbar. A note indicating that the domain is in Passive Mode is added to Policy Manager as shown below, so that you always know when a domain is in passive mode.



2. The note also allows you to specify the syslog/audit action that you want to use while the domain is in passive mode. Select the appropriate radio button:
  - Syslog only - a syslog message is generated when a rule is used.
  - Audit Trap only - an audit trap is generated when a rule is used.
  - Both - both a syslog message and an audit trap are generated when a rule is used.
  - Rule Specified - Generate a syslog message or audit trap or both, as specified for each rule in the rule's [General tab](#).
3. Select **File > Enforce Preview**. The Enforce Preview window opens.
4. Select "Show All" and then select the Matrix Platinum device folder.
5. In the Enforce Preview window, you will see rules listed in the Excluded section, with "Passive Mode" appended to each rule name. These rules will not be enforced because their actions are not allowed in Passive Mode. Rules in the Included section will be enforced because their actions specify the syslog/audit actions that are allowed in Passive Mode.
6. Click the **Enforce** button in the Enforce Preview window to enforce the domain (in passive mode) to your network.
7. Review the syslog and/or audit trap data collected while in passive mode to verify that traffic is being handled appropriately by the policy rules. Make any changes as needed. When you are confident the domain configuration is working effectively for your network, deselect the passive domain mode option and enforce the policy domain to your network.

---

## Related Information


For information on related tabs:

- [General Tab \(Rule\)](#)

## How to Filter, Find, and Sort

---

Use the following instructions to perform filter, find, and sort operations on column entries in Policy Manager right-panel tables.

**NOTE:** Some Policy Manager tables use a set of Table Tools to find, filter, sort, print, and export information in a table. You can access these Table Tools by clicking the Table Tools  button in the upper left corner of the table. For more information, see Table Tools.

Instructions on:

- [Filtering](#)
- [Finding](#)
- [Sorting](#)

### Filtering

When the information in the right panel is presented in a column format, you can perform a filter so that only those entries matching your filter criteria will be displayed. You can filter the entries in a single column or in all columns, and you can apply consecutive filters.

1. Select **View > Filter**. You can also right-click on a column header, and select **Filter**. The Filter window opens.
2. In the **Filter** field, enter the numeric value or text you want to filter.
3. Click the **Case Sensitive** check box to filter based on the exact case of the text entered in the **Filter** field.
4. Click the **Match Whole Word** check box to filter based on the entire value or text entered in the **Filter** field.
5. From the **Column** drop-down list, select the column you want to filter. If you select **All Columns**, the filter criteria will be applied to all entries.
6. If you have already performed a filter, click the **Whole Table** option to perform a new filter on all entries instead of just the filtered entries. Or, click the **Current Table** option to perform a new filter on the results of the previous filter.
7. Click **Filter**.

All entries that do not match the filter criteria will be removed. You can apply additional filters by repeating steps 2 - 7, or revert to the unfiltered entries by selecting **Show All**.

## Finding

When the information in the right panel is presented in a column format, you can search for a specific value in a single column or in all columns. You can search forward or backward from your current position, and also restrict your search to match the exact case and/or whole word of the entry.

1. Select **Edit > Find**. You can also right-click on a column header, and select **Find**. The Find window opens.
2. In the **Find** field, enter the value or text you want to search for.
3. Click the **Case Sensitive** check box to search based on the exact case of the text entered in the **Find** field.
4. Click the **Match Whole Word** check box to search based on the entire value or text entered in the **Find** field.
5. In the Direction box, select the direction in which you want to search: **Forward** (top to bottom) or **Backward** (bottom to top).
6. From the **Column** drop-down list, select the column you want to search. Select **All Columns** to search all entries.
7. Click **Find**.

The matching entry is highlighted in the right panel. Click **Find** again to search for another entry matching the search, or select **Clear** to clear the value in the **Find** field and enter a new search criteria.

## Sorting

When the information in the right panel is presented in a column format, you can sort the column entries in ascending or descending order. Text fields are sorted alphabetically, numeric fields are sorted numerically, and mixed fields are sorted alpha-numerically.

1. Select **View > Sort**. The Sort window opens.
2. From the **Column** drop-down list, select the column you want to sort.
3. In the Direction box, select the order in which you want to sort the list:

**Ascending** or **Descending**.

4. Click **Sort**.

The entries will be reordered based on the sort criteria.

**Tip:** You can also sort a column by right-clicking on a column header and selecting **Sort Ascending** or **Sort Descending**.

---

## **Related Information**


For information on related windows:

- [Filter Window](#)
- [Find Window](#)
- [Sort Window](#)



## How to Freeze/Unfreeze a Port

---

Freezing a port enables you to "lock" it so that no one can accidentally reconfigure sensitive attributes such as port authentication or default role settings. For example, if a port is frozen and the administrator later assigns a default role to the entire device, the frozen port will not receive the new default role. To reconfigure a frozen port, you must clear its frozen status, do the configuration, then freeze it again. One application of this feature would be to prevent interswitch link ports from being accidentally reconfigured. You can tell if a port is frozen or not by looking at the port icon  or by checking the Frozen Status on the [Port Properties General tab](#).

The Frozen Port feature is a *software* feature available in Policy Manager. It does not freeze the ports in the switch firmware itself, but protects the user from making configuration changes to sensitive ports using the software application. Therefore, setting a port to be frozen in Policy Manager will not automatically set the port to be frozen in other NetSight applications.

You can freeze ports as part of the general port configuration process in the [Port Configuration Wizard](#), or you can freeze or clear frozen ports on an individual or selected port basis.

You cannot terminate sessions on frozen ports.

Instructions on:

- [Freezing/Unfreezing a Port](#)
- [Freezing/Unfreezing a Device](#)

### Freezing/Unfreezing a Port

To freeze or clear a single port:

The quickest way to freeze a single port or clear it is to select the port and use the right-click menu **Set Frozen** or **Clear Frozen** options.

1. In the left-panel Network Elements tab, select the device where the port resides and expand the slot or ports grouping in the right-panel Details view.
2. Right-click the port you want to freeze or unfreeze, and select **Set Frozen** or **Clear Frozen**.

You can also freeze a port or clear a port's frozen state on the [Port Properties window General tab](#).

**NOTE:** You can freeze multiple ports or clear them by holding down the **Shift** or **Control** key while selecting the ports in the right panel.

## Freezing/Unfreezing a Device

You can freeze all the ports on a single device or clear them by selecting the device and using the right-click menu **Set Frozen** or **Clear Frozen** option.

To freeze or unfreeze an entire device:

1. In the left panel, select the Network Elements tab.
  2. Right-click the device whose ports you want to freeze or unfreeze.
  3. To freeze all the device's ports, select **Set Frozen**. To unfreeze all the device's ports, select **Clear Frozen**.
- 

### Related Information

For information on related windows:

- [Port Properties - General Tab](#)

For information on related tasks:

- [How to Configure Ports](#)

## How to Import From Device

---

Use the Import From Device Wizard to import roles and rules from a selected device or devices into your Policy Domain configuration. This feature is useful when:

- you need to rebuild a domain configuration. You can import roles and rules already enforced on a device into a new domain.
- you are creating your first domain configuration. You can import existing static classification rules on a device into the domain, saving the time it would take to duplicate the rules through Policy Manager.

Using the wizard, you can import roles and rules, and easily organize the rules into services. You can create new services, and merge the imported rules into these new services or into any existing services in your current domain.

### Using the Import From Device Wizard

1. Select **File > Import > Policy Configuration From Device**. The Import From Device Wizard opens.

#### *Import From Device*

2. Select whether you would like to import roles and/or rules from the device (s):
  - **Roles** – Select this option to import roles, including the role’s name, description, default VLAN (access control), and default class of service.
  - **Rules** – Select this option to import the traffic classification rules associated with any roles on the device. If you select this option, you can also select whether to import any static traffic classification rules configured on the device.

---

**NOTE:** If you import a device-specific rule, it will be converted to a rule type of "All Devices." If you want the rules to be device-specific, you will have to change their Rule type via the Rule General tab after the import and prior to Enforce.

---

3. Select the **Class of Services** checkbox to import all role-based Class of Service information including Class of Services, corresponding role-based

rate limit port groups, and mapped role-based rate limits. Selecting this checkbox will also give you the opportunity import the GVRP status (via a dialog box during the import) as long as the domain status is not set to Ignore and it does not match the GVRP status read from the device during the import.

---

**WARNING:** If Global Services are used, then modifying Class of Service data (which may be used by Global Services and Rules) can potentially change the policy configuration for **all domains**. To avoid this, perform the Import Policy Configuration From Device operation on a domain that has the "Edit > Do Not Use Global Services" option checked.

---

4. Click **Next**.

### *Device Selection*

5. This window lets you select the devices you would like to import from. The Devices panel on the left side of the window displays all the devices and device groups in the current domain. Select the devices that you would like to import from, and click **Add** to list them in the Selected Devices panel. You can also create or import new devices from which to read policy. Click the **Create** button to add a new device, if desired. Click the **Import from Data File** button to open a window where you can select a data file to import devices from. If you use these methods, you can use the **Remove the created/imported Devices from Policy Manager upon completion** checkbox if you don't want the devices permanently added to the domain.
6. If you selected the **Class of Services** checkbox in the previous window, you must specify the device from which to import the Class of Service information. Since different devices may specify different CoS configurations for the same Class of Service, a single device must be specified. The existing Classes of Service (in the domain) will be updated with the CoS information from this one device. However, in the case of the Class of Service **Mode** which is a per-device attribute (specified in the Device General tab), only the devices selected here in this window will have their Class of Service Mode updated (in the domain) to match the mode on the actual device.
7. Click **Next**.

### *Read From Device*

8. This view displays all the roles and rules available for import into your domain. Using the checkboxes in the Selected columns, select the roles and

rules that you want to add to your domain. You can sort the tables by clicking on a column heading.

### Roles Panel

The top panel lists all the roles you can select from, along with information on the role's default actions including access control and class of service. If the role already exists in your domain, it cannot be imported. In addition, any differences between the existing role in your domain and the same role on the device will be indicated using red text, except device-level and port-level mappings.

- **Selected** - Use the checkboxes to select the roles you want to add to your domain. Roles that already exist in your current domain display "exists" in this column, and cannot be selected.
- **Name** - The name of the role.
- **Access Control** - The [default access control](#) associated with the role. If the role does not have default access control, the column will display N/A.
- **CoS** - The [default class of service](#) associated with the role. If the role does not have default class of service, the column will display N/A.
- **Syslog** - Displays whether the syslog functionality (a syslog message is generated when the role is used) is configured as a default action of the role.
- **Audit Trap** - Displays whether the audit trap functionality (an audit trap is generated when the role is used) is configured as a default action of the role.
- **Disable Port** - Displays whether the disable port functionality (ports reported as using this role will be disabled) is configured as a default action of the role.
- **Traffic Mirror** - Displays whether [traffic mirror](#) functionality is configured as a default action of the role.
- **TCI Overwrite** - Displays whether [TCI Overwrite](#) is enabled or disabled for the role.
- **Device(s) of Origin** - The device(s) the role exists on.

### Rules Panel

The bottom panel lists all the rules you can select from, along with information on each rule's traffic description (type and value) and actions

(access control and class of service). You can select a checkbox to allow the wizard to **Consolidate IP TCP/UDP Rules** containing adjacent ports and equal actions into ranges where possible. This will reduce the number of rules imported into your domain. For example, if a device has two UDP Port Destination rules - one for FTP (port 21) and one for FTP Data (port 20) - if this checkbox is selected, a range rule of 20-21 is created instead of two separate rules.

- **Selected** - Use the checkbox to select the rules you want to add to your domain. Rules that already exist in your current domain display "exists" in this column, and cannot be selected.
- **Name** - The name of the rule, generated from the rule's actions, type, and value.
- **Cleanup Static** - If you are importing static rules, select this checkbox if you want the wizard to clear the static rule from the port tables on the device. It is recommended that you cleanup static rules so they do not interfere with the rules set through Policy Manager.
- **Type** - The Classification Type for the rule.
- **Value** - The classification value.
- **Access Control** - The [access control](#) associated with the rule. If the rule does not specify access control, this column will display N/A.
- **CoS** - The [class of service](#) associated with the rule. If the rule does not specify a class of service, this column will display N/A.
- **Syslog** - Displays whether the syslog functionality (a syslog message is generated when the rule is used) is enabled, disabled, or prohibited for the rule.
- **Audit Trap** - Displays whether the audit trap functionality (an audit trap is generated when the rule is used) is enabled, disabled, or prohibited for the rule.
- **Disable Port** - Displays whether the disable port functionality (ports reported as using this rule will be disabled) is enabled, disabled, or prohibited for the rule.
- **Traffic Mirror** - Displays whether the [traffic mirror](#) functionality is enabled, disabled, or prohibited for the rule.
- **TCI Overwrite** - Displays whether [TCI Overwrite](#) is enabled, disabled, or prohibited for the rule.
- **Role(s) of Origin** - The role the rule is coming from.

9. Click **Next**.

### *Organize and Update*

10. The wizard provides a selection of common ways to organize the rules into services. Select one of these options:
  - All Rules in one Service - Organize all the imported rules into one new service.
  - Rules placed in Services by Action - Organize all imported rules by their action: Deny, Permit, Contain, or Prioritize
  - Rules placed in Services by Classification Layer - Organize all imported rules by their Traffic Classification Layer: Layer 2, Layer 3, or Layer 4.
  - Rules placed in Services by Classification Type - Organize all imported rules by their Traffic Classification Type.
  - Rules placed in Services by Role of Origin - Organize all imported rules by the name of the role they originated from. If desired, you can add these services to the corresponding role in the domain by selecting the **Add Generated Services to Matching Role** checkbox.
11. In the Role Update section, select the checkbox if you would like to update the existing roles in your domain with any conflicting role information read from the device(s). If the role already exists in your domain, it cannot be imported. However, this option lets you update the existing role in your domain with the values of the same role read from the device(s). These differences were highlighted in the [Read From Device](#) role panel in red text. (Device-level and port-level mappings will be imported even though they are not highlighted as differences.)
12. Click **Next**.

### *Merge Rules*

13. In this view, the panel on the left shows the rules organized into generated services as specified in the previous view. The panel on the right shows the current set of services available in your domain. You can merge the rules into your available services, or leave the rules as organized in the previous view. To merge the rules:
  - a. In the left panel, select the rules and/or services you want to merge.
  - b. In the right panel, select the service you want to merge the rules into.

- c. Click the **Add** button. The rules will be reorganized under the service.
  - d. If desired, you can create a new service. Click **Create Service** to open a window where you can name a service and add it to the Available Services panel.
14. Because you are importing new rules into existing services, there is a possibility of conflicts between the new rules and any existing rules in a service. For example, two rules might have the same traffic descriptor but forward traffic to different VLANs, or have different priorities. If the two rules are applied to the same service, or to the same role via two different services, unpredictable and undesired behavior could result. Click **Check for Conflicts**, and Policy Manager will check rule traffic descriptions and action values, and provide a message if conflicts are found. This gives you an opportunity to resolve the conflicts prior to importing. Any conflicting rules that are not resolved will be disabled when the import is performed.
  15. When your rules are organized as desired, click **Finish** to perform the import.

---

**NOTE:** Because the import operation imports only roles and rules from the device (not the complete policy configuration), a Verify operation performed following the import may fail. Also, when you import device-specific rules, these rules are converted to a Rule Type of "All Devices," and this will cause Verify to fail. If you want the rules to be device-specific, you will have to change their Rule Type via the Rule General tab after the import and prior to Enforce.

---

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)



## How to Initialize the Policy Manager Database

---

Policy Manager provides a way for you to initialize only the Policy Manager components in the NetSight Database. The initialize operation removes **all** Policy Manager domains and domain data from the database including:

- Roles, services, service groups, and rules
- Devices assigned to the domains (the devices are not deleted from Console)
- Port groups
- VLANs
- User-defined classes of service (CoS) and rate limiting

Using this operation instead of the Restore Initial Database function (accessed in the Server Information window) allows you to initialize your Policy Manager components while retaining your NetSight Console and other NetSight application data elements in the database.

---

**CAUTION:** -- It is recommended that you make a backup of your NetSight Database prior to performing the initialize operation using the Backup Database window accessed from the Server Information window.  
-- The capability to restore or initialize a database is a NetSight Suite capability and is not affected by whether the user has read/write capabilities in Policy Manager. This means that when creating read-only users for Policy Manager, it is important to remove the initializing database suite capability as well, so that the users will not have the ability to delete the database.

---

1. Make a backup of your database using the Backup Database window accessed from Database tab in the Server Information window (Tools > Server Information.)
2. Select **File > Database > Initialize PM Components** to begin the initialize operation. You will see a message asking if you want to delete all Policy Manager data in the server's database. Click **OK**.

## How to Lock MAC Addresses to Ports

---

MAC Locking ensures that only specific MAC addresses can access a port, and that traffic from any other MAC addresses will be discarded. There are two kinds of MAC Locking: Dynamic and Static. When you enable Dynamic MAC Locking on a port, the next MAC address that authenticates or accesses the port (up to the maximum number of dynamic locked MAC addresses allowed) will have exclusive access to that port from that time on. Static MAC Locking lets you create a list of locked MAC addresses for a port so that the port only accepts traffic from those MAC addresses.

In order for MAC Locking to take effect on a port, it must be enabled on the port and at the device level. You can enable MAC Locking for a specific port using the [Port Properties window MAC Locking Tab](#), and enable MAC Locking for the device on the [MAC Locking Tab \(Device\)](#), or in the [Device Configuration wizard](#). You can also enable MAC Locking for multiple ports in the [Port Configuration wizard](#). MAC Locking is only available on devices that support it, and is not allowed on backplane and logical ports.

Instructions on:

- [Dynamic MAC Locking](#)
- [Static MAC Locking](#)

### Dynamic MAC Locking

When Dynamic MAC Locking is enabled on a port, the next MAC address that authenticates or accesses the port (up to the maximum number of dynamic locked MAC addresses allowed) will have exclusive access to that port. Use the [Port Configuration Wizard](#) to enable Dynamic MAC Locking on multiple ports, or follow these steps to enable it on a single port.

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click on a port and select **Properties** from the menu. In the Port Properties window, select the [MAC Locking tab](#) (in the top row of tabs).
3. Select the [General sub-tab](#).
4. Enable MAC Locking on the port. If the device does not support MAC locking, this option is grayed out.

5. In the MAC Locking Limits area, set the maximum number of MAC addresses that can be locked dynamically on the port. The numbers in parentheses let you know the range of allowed values for the particular port.
6. Click **Apply**.

## Static MAC Locking

Static MAC Locking lets you create a list of locked MAC addresses for a port so that the port only accepts traffic from those MAC addresses. You can add Static MAC Locking to a single port or multiple ports.

### *On a Single Port*

1. Select a device in the left-panel Network Elements tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click on a port and select **Properties** from the menu. In the Port Properties window, select the [MAC Locking tab](#) (in the top row of tabs).
3. Select the [General sub-tab](#).
4. Enable MAC Locking on the port. If the device does not support MAC locking, this option is grayed out.
5. In the MAC Locking Limits area, set the maximum number of static MAC addresses that can be locked on the port. The numbers in parentheses let you know the range of allowed values for the particular device. Click **Apply**.
6. You can move all Dynamic Locked MAC addresses (with the Locking Cause of "First Arrival") to Static Locked MAC addresses by clicking the **Apply** button in the Static MAC area. Make sure that the **Maximum Number of Static Locked MAC Addresses** is set to a large enough value to accommodate all the addresses.
7. In the [Locked MAC Addresses sub-tab](#), click **Retrieve** to populate the Locked MAC Addresses table with a list of the MAC addresses currently locked on the selected port.
8. Click the **Add** button to open the [Add Static MAC window](#) where you can add to the list of locked MAC addresses for the port.
9. In the Add Static MAC window, the Detected MACs table lists the addresses detected on the selected port and their corresponding index number.

10. In the Detected MACs table, [select](#) the desired MAC address(es) and click **Add** to list the address(es) in the Statically Add MACs list. You can also enter a MAC address and index number, then click **Add** to add the address to the Statically Add MACs list. To remove an address from the Statically Add MACs table, [select](#) the address(es) and click **Remove**.
11. Click **OK**.

### *On Multiple Ports*

1. In the Network Elements tab, select a single device, a device group, or the All Devices folder.
2. Select the MAC Locking tab in the right panel, and click **Retrieve** to display the current list of locked MAC addresses for the selected device(s) or port group. (If the device does not support the MAC locking feature, the **Retrieve** and **Add** buttons are grayed out.)
3. You can move all Dynamic Locked MAC addresses (with the Locking Cause of "First Arrival") to Static Locked MAC addresses by clicking the **Apply** button in the Static MAC area. To ensure that all Dynamic Locked MAC addresses are changed to Static, make sure that the **Maximum Number of Static Locked MAC Addresses** is set to a large enough value in the [Port Properties window MAC Locking Tab](#).
4. Click the **Add** button to open the [Add Static MAC window](#) where you can create a list of locked MAC addresses.
5. In the Add Static MAC window, the Detected MACs table lists the addresses detected on the selected device(s) and their corresponding index number and device IP address. (Only MAC addresses for devices that support MAC Locking are displayed.) If you have selected a single device in the left-panel tree, the Device column in the table is not displayed.
6. In the Detected MACs table, [select](#) the desired MAC address(es) and click **Add** to list the address(es) in the Statically Add MACs list. You can also enter a MAC address and index number, and select a device from the dropdown list, then click **Add** to add the address to the Statically Add MACs list. (If you have selected a single device in the left-panel tree, the Device dropdown list is not displayed.) To remove an address from the Statically Add MACs table, [select](#) the address(es) and click **Remove**.
7. Click **OK**.

## Related Information

For information on related concepts:

- [MAC Locking](#)

For information on related tasks:

- [Using the Device Configuration Wizard](#)
- [Using the Port Configuration Wizard](#)

For information on related windows:

- [Add Static MAC Window](#)
- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(My Network/AllDevices Folder\)](#)
- [MAC Locking Tab \(Device Group\)](#)
- [Port Properties - MAC Locking Tab](#)
- [MAC Locking Tab \(Port Group\)](#)

## Rule Accounting and Rule Hit Reporting

---

Rule accounting and rule hit reporting provide the ability to collect data on how policy rules are being used on your network. Once you have configured the accounting and reporting functionality, you can view the rule usage data that is collected using the Rule Usage tabs or the Policy Rule Hit Reports.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. This information is displayed in the right-panel Rule Usage tabs. When Policy Rule Hit Reporting is also enabled, then rule hit data is also collected through syslog messages sent from the devices and stored in the NetSight database. This information is then displayed in the Policy Rule Hit Reports available from the View menu and the Rule Usage tabs.

Instructions on:

- [Configuring Rule Accounting and Reporting](#)
- [Viewing Rule Usage Information](#)
- [Viewing Policy Rule Hit Reporting](#)

## Configuring Rule Accounting and Reporting

Use the following steps to enable rule accounting on a device and configure the rule accounting and rule hit reporting parameters.

---

**NOTE:** Rule accounting is used to show if a given rule has been used to classify traffic on a device, and on which port the rule hit occurred. When a rule is used on a port, an entry is made in the rule hit table. Subsequent rule hits do not alter this entry in the rule hit table, however you can use the "clear rule usage" options discussed below to customize the table to indicate how recently, or in what context, these rule hits have occurred. You can specify that a rule hit is cleared when the port link-status changes, when the role which defines the rule is assigned via a Role Mapping, and/or according to a set interval. Based on these options, you can determine how fresh your rule hit data is, and/or what the rule hit data is within a specific session. For example, if you specify a clear rule usage interval of 30 minutes, then you know that any rule hits displayed in the Rule Usage tab (after you click Retrieve) have been reported in the last 30 minutes. These clear rule usage options also control the frequency that the syslog messages containing the rule hit data are sent from the device for rule hit reporting.

---

**TIP:** Use the [Device Configuration Wizard](#) to enable Rule Accounting and reporting on multiple devices.

---

1. Select a device in the left-panel Network Elements tab, and click the [Role/Rule tab](#) in the right panel. (If a device does not support the Rule Accounting feature, the rule accounting options will be grayed out.)
2. In the Rule Accounting section, enable **Rule Accounting**.
3. Enable the **Use Expanded Format for Rule Hit System Log Messages** option. When enabled, the device will provide additional information in Policy Rule Hit syslog messages. For example, the additional information may include what actions may have been initiated by the rule (if any).
4. Enable the **Clear Rule Usage on Port Link-Status Change** option if you want to clear rule usage data when the port has a link-status change when a user connects or disconnects.
5. Enable the **Clear Rule Usage on Role Mapping Change** option if you want to clear rule usage data when there's a role-mapping change. If a role-mapping is defined and traffic comes onto the device and is mapped to the defined role, then all rules in that role will have their rule hit data cleared. This option should be enabled for Policy Rule Hit Reporting. It allows you to start a new data collection when the name of the role changes on the port, providing for a cleaner data presentation.
6. For Policy Rule Hit Reporting, select the **Enable Syslog Server** checkbox to set up the device to send syslog messages.
7. In the Clear Rule Usage on Interval section:
  - a. Enable the **Clear Rule Usage on Interval** option to clear the rule usage data at a set interval. This option should be enabled for Policy Rule Hit Reporting because it specifies the interval at which syslog messages will be sent to the server, thereby providing data samples at even intervals.
  - b. Enter the desired interval (in minutes).
  - c. Click **Apply**.
8. The **Rule Usage Auto Clear Ports** list must contain all ports where you want rule accounting to take place. If you have enabled any of the clear rule usage options, this list must specify the ports on the device where the clear operations will be performed. Click **Add/Remove** to open the [Add Ports window](#) where you can select ports to add to the list. Click **Apply** to set any changes you have made.

9. For each rule that you want to collect rule hit data on, you must specify the action to take place when a "rule hit" is reported. Select a rule in the left-panel Services tab, then select the [Rule General tab](#) in the right panel. In the Actions section, select the desired actions to take place when this rule is used:

- Generate System Log on Rule Hit - A syslog message is generated when the rule is used. This option must be selected for Policy Rule Hit Reporting.

---

**NOTE:** N-Series devices with firmware version 6.x or earlier must be added to a policy domain using the switch IP address and not the router IP address. This is because syslog messages contain the switch IP address, and this IP address must be found as a modeled device in a policy domain in order to match the rule to the domain's rule set. If a match is not found, the rule hit won't be written to the database.

---

- Generate Audit Trap on Rule Hit - An audit trap is generated when the rule is used.
  - Disable Port on Rule Hit - Any port reported as using this rule will be disabled.
- 

**TIP:** You can also specify these rule usage actions when you create a rule using the [Rule Wizard](#).

---

You are now ready to view rule usage and rule hit reporting information.

## Viewing Rule Usage Information

Rule usage information provides a current snapshot of rule hits on a device. When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. This information is displayed in the Rule Usage tabs.

- **To view the ports that a specific rule has been used on.**  
Select a rule in the left-panel Services tab, then select the [Rule Usage tab](#) in the right panel. (If the rule type does not include any devices that support rule accounting, this tab will be grayed out.) Click the **Retrieve** button to display the ports where the rule was used. Use the **Clear** button to clear selected port(s) from the rule's usage list.
- **To view the rules that have been used for a specific role or service, or on a specific device or port.**  
Select a role, service, device, or port in the left-panel tree, then select the



[Rule Usage tab](#) in the right panel. Click the **Retrieve** button to display the rule usage information. Use the **Clear** button to clear selected port(s) from the associated rule's usage list.

- **To view any ports on a device that have been disabled due to rule usage.** Select a device in the left-panel Network Elements tab, and click the [Role/Rule tab](#) in the right panel. Click the **Retrieve** button to display any disabled ports. Use the **Clear** button to clear any selected disabled ports, and re-enable them. Keep in mind that if the port continues to receive traffic that matches the rule, and the rule is still configured to disable the port, then the port will almost immediately reappear in the table.

## Viewing Policy Rule Hit Reporting

Policy Rule Hit Reporting provides a historical look at rule usage over time for domains. When rule accounting is enabled on a device, the Policy Rule Hit data is collected through syslog messages sent from the device to the NetSight server and stored in the NetSight database. This information is displayed in Policy Rule Hit Reports.

- **To view the rule hits for all devices in all domains as they are being received.** From the Policy Manager View menu, select View > Policy Rule Hit > Real Time Policy Rule Hits. This table displays real-time policy rule hits for all domains as they are being collected in the database. Viewing rule hits lets you know that rule hit data is being successfully collected. The "Time Received" column reflects the time the rule hit was received by the NetSight server. The **Clear** button empties the display table only. A right-click menu allows the report to be printed or exported to a file.
- **To view rule hit data on a polling cycle.** From the Policy Manager View menu, select View > Policy Rule Hit > Policy Hit Accounting Tool. This tool shows the rule hits read from the database on a polling cycle. The data can be filtered by device and by the type of rules (all rules, hit rules, permit or discard rules). The graph is a bar chart and you can select to show rules, services, service groups, or roles. A right-click menu allows the graph to be printed or exported to a file. The polling interval is set in the [Policy Rule Hit Reporting options](#) panel.
- **To view the top-10 rules used in the domain in the last 24 hours.** From the Policy Manager View menu, select View > Policy Rule Hit > Top-

10 Policy Rule Hits (24 hours). The first chart shows the top ten rules in the current domain based on the last 24-hour period. The second chart shows an individual rule's usage mapped out by role along with a table that shows all the individual rule hits that make up the data for the second chart. The **Retrieve** button updates the report with data for the period ending with the current time. A right-click menu allows the report to be printed or exported to a file.

- **To view the top-10 rules used in the domain in the last week.**

From the Policy Manager View menu, select View > Policy Rule Hit > Top-10 Policy Rule Hits (1 week). The first chart shows the top ten rules in the current domain based on the last 7-day period. The second chart shows an individual rule's usage mapped out by role along with a table that shows all the individual rule hits that make up the data for the second chart. The **Retrieve** button updates the report with data for the period ending with the current time. A right-click menu allows the report to be printed or exported to a file.

- **To view rule usage trends in the domain in the last week.**

From the Policy Manager View menu, select View > Policy Rule Hit > Rule Usage Trend (1 week). This report shows the top five rules with the most rule hits in the current domain based on the last 7-day period. The first chart shows rule usage mapped out by time. The second chart shows an individual rule's usage mapped out by role along with a table that shows all the individual rule hits that make up the data for the second chart. The **Retrieve** button updates the report with data for the period ending with the current time. A right-click menu allows the report to be printed or exported to a file.

- **To view rule hit data filtered on a role, service, rule, device, slot, or port.**

- Select a role, service, rule, device, slot, or port in the left-panel tree, right-click and select Policy Rule Hits from the menu. This report shows the last 100 rule hits for the selected item. The **Clear** button empties the display table only.
- Select a role, service, rule, device, slot, or port in the left-panel tree, right-click and select Top-5 Rule Usage Trend (1 week) from the menu. This report shows the top five rules with the most rule hits based on the last 7-day period for the selected item. The **Clear** button empties the display table only.

## Related Information

For information on related tasks:

- [Using the Device Configuration Wizard](#)
- [Using the Classification Rule Wizard](#)

For information on related tabs:

- [Role/Rule Tab \(Device\)](#)
- [Port Properties - Rule Usage Tab](#)
- [Rule Usage Tab \(Role/Service/Device\)](#)
- [Rule Usage Tab \(Rule\)](#)

## How to Select on Add/Remove Windows

---

Policy Manager includes several Add/Remove windows in which you can add items from a left panel to a right panel, and remove items from the right panel. The following procedures explain how to make single and multiple selections in the panels and move the selections to the opposite panel.

Instructions on:

- [Selecting single items](#)
- [Selecting multiple sequential items](#)
- [Selecting multiple non-sequential items](#)

### Selecting single items

To select one item from the left panel and add it to the right panel, use one of these methods:

- Double-click the item.
- Click the item, then click **Add**.
- Click and drag the item to the right panel.

To remove one item from the right panel, use one of these methods:

- Double-click the item.
- Click the item, then click **Remove**.

### Selecting multiple sequential items

To select a sequence of items in the left panel and add them to the right panel:

1. Hold down the **Shift** key and click the first and last (or last and first) items in the sequence.
2. Click **Add**.

To remove a sequence of items from the right panel:

1. Hold down the **Shift** key and click the first and last (or last and first) items in the sequence.
2. Click **Remove**.

## Selecting multiple non-sequential items

To select multiple non-sequential items in the left panel and add them to the right panel:

1. Hold down the **Ctrl** key and click each item you want to add.
2. Click **Add**.

To remove multiple non-sequential items from the right panel:

1. Hold down the **Ctrl** key and click each item you want to remove.
2. Click **Remove**.

# How to Set Policy Manager Options

---

Use the Options window (**Tools > Options**) to set options for the Policy Manager application. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Policy Manager folder in the tree to view all the different options you can set.

Instructions on setting the following Policy Manager options:

- [Default Class of Service](#)
- [Dialog Boxes](#)
- [Name Resolution \(PM\)](#)
- [Optional Views](#)
- [Policy Rule Hit Reporting](#)
- [Ports](#)
- [Startup](#)
- [SNMP Options](#)
- [Tab Configuration](#)
- [Welcome View](#)
- [Wireshark](#)

## Default Class of Service

Use the [Default Class of Service view](#) to specify the default Class of Service mode to set on a device (if supported) when it is created in Policy Manager or added to the domain via the Assign Devices to Domain window. The default setting is "Role-Based Rate Limits/ Transmit Queue Configuration." The CoS mode is written to the devices when an Enforce operation is performed. This setting applies to all users.

**NOTE:** You can change this default value for a specific device by setting a different CoS mode in the [Device General tab](#) or via the Device Configuration Wizard.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Policy Manager folder and select Default Class of Service. The right-panel Default Class of Service view is displayed.

3. Select the class of service mode or select the option to disable rate limits on the device. Only certain devices such as the N-Series Gold and Platinum devices support both modes, but you cannot have both modes enabled at the same time. See [Getting Started with Class of Service](#) for more information.
  - Rate Limits Disabled - Select this option if you want rate limits disabled. This means that any priority-based rate limits will not be written to devices on enforce, and any role-based rate limits will not be included in roles written to devices on enforce.
  - Role-Based Rate Limits/Transmit Queue Configuration - Select this mode if you want to be able to configure role-based rate limits and transmit queues on devices. These rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the class of service. See [How to Define Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.
  - Priority-Based Rate Limits - Select this mode if you want to configure priority-based rate limits for use with legacy devices such as the E7 and E1 devices. See [Priority-Based Rate Limits](#) for more information.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Dialog Boxes

Use the [Dialog Boxes view](#) to turn on the message dialog boxes that you have turned off on individual dialog box(es). 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 Policy Manager folder and select Dialog Boxes. The right-panel Dialog Boxes view is displayed.
3. In the Ignored Dialog Boxes section, click the **Re-Show All** button to turn on the display of messages that have been turned off in individual message dialog box(es).
4. Click **OK** to set the option and close the window. Click **Apply** to set the option and leave the window open.

## Optional Views

Use [Optional Views](#) to choose whether or not you want certain views to be displayed. These settings apply 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 Policy Manager folder and select Optional Views. The right-panel Optional Views view is displayed.
3. Select the **Show Enforce Preview on Enforce** checkbox if you want the [Enforce Preview window](#) to appear any time you [enforce](#), before the actual enforcement takes place. You can also turn this option on and off on the Enforce Preview window itself.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Name Resolution (PM)

Use the [Name Resolution \(PM\) view](#) to enable or disable host name resolution for Policy Manager Port Usage tabs and Anti-Spoofing binding views.

Host name resolution must also be enabled globally in the Suite Options > Name Resolution panel or these settings are ignored.

These options are enabled by default, but can be turned off for diagnostic or troubleshooting purposes, if needed.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Policy Manager folder and select Name Resolution (PM). The right-panel Name Resolution (PM) view is displayed.
3. Enable or disable the options as desired.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Policy Rule Hit Reporting

Use the [Policy Rule Hit Reporting view](#) to configure the Policy Rule Hit Reporting feature. This feature allows you to view reports on rule usage for your policy domains. The reports can be accessed from the View menu. To use rule hit reporting, the devices must be configured to do rule accounting via the device [Role/Rule tab](#), and each rule in the domain must have the Generate System Log



on Rule Hit option selected on the rule [General tab](#). For more information on configuring Policy Rule Hit Reporting, see [Rule Accounting and Rule Hit Reporting](#).

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Policy Manager folder and select Policy Rule Hit Reporting.
3. Specify the **Database Aging Row Count**. Once every 24 hours (based on when the server is started), the policy rule hit database table is trimmed to no more than the row count (number of entries) specified here. This prevents the table from getting too large. This setting is for all users.
4. Specify the **Syslog Message Queue Drain Size**. This is the maximum number of rule hits written to the database by the reporting agent every two seconds. The reporting agent has a message queue that stores all the rule hits from the syslog server. Every two seconds the queue is drained and the messages are written to the database. The Syslog message drain queue size limits the number of rule hits that can be written to the database. This prevents the reporting agent from monopolizing the database in the case of a deny attack on the network, where many rule hits could be generated at one time. This setting is for all users.
5. Specify the **Real Time View Maximum Table Size**, which is the maximum number of rows that can be added to the Real Time Rule Hit view. The oldest rows are aged out when new ones come in. This setting is for the current user only.
6. Specify the **polling interval** for the Policy Rule Hit Accounting tool. This tool shows all rule hits read from latest data in the database and can be accessed by selecting the View menu > Policy Rule Hit > Policy Accounting Tool. The polling interval is the frequency of the database query. This setting is for the current user only.
7. Specify the **Policy Accounting View Maximum Table Size**, which is the maximum number of rows allowed in the tables displayed in Policy Rule Hit Reports (View > Policy Rule Hit). The oldest rows are aged out when new ones come in. This setting is for the current user only.
8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Ports

Use the [Ports view](#) to set or clear the Hide Logical Ports feature. The feature is set by default when you first launch Policy Manager. This setting applies only to the current user.

The Hide Logical Ports feature lets you hide the display of logical ports in Policy Manager. Logical ports include SmartTrunk ports and LEC (LAN emulation client) ports, which can be seen in Policy Manager even if they are not yet configured or connected. If there are too many of these logical ports, they can cause unwanted clutter in your Policy Manager port list displays.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Policy Manager folder and select Ports. The right-panel Ports view is displayed.
3. Use the checkbox to enable or disable the **Hide Logical Ports** feature, as desired.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Startup

Use the [Startup view](#) to configure the features that run on Policy Manager startup.

When you launch Policy Manager or open a domain, two background operations are automatically performed: a background read of the VLANs from all reachable devices and a background verify operation that determines if the roles on the devices match those in the current Policy Manager domain. Because these operations run in the background, you have instant access to Policy Manager and the domain even while the operations are verifying the current status of the domain. However, you can deselect the options in this view to prevent these operations from being performed, if desired. (For more information on the verify operation, see [Verifying](#) in the Policy Manager Concepts file.)

In addition, you can set an option that allows you to select a domain on startup. When you start Policy Manager, the Select a Domain to Open window presents a drop-down list that allows you to select which domain to open, or create a new domain, if desired. If this option is not selected, Policy Manager will open the domain that was open when the NetSight client last closed.

These settings apply 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 Policy Manager folder and select Startup. The right-panel Startup view is displayed.
3. Deselect the **Background Verify on Startup/Domain Open** checkbox to stop a background verify operation that is performed when Policy Manager is launched or when you open a domain.
4. Deselect the **Background Get VLANs on Startup/Domain Open** checkbox to stop a background operation to read the VLANs from all reachable devices that is performed when Policy Manager is launched or when you open a domain.
5. Select the **Select a Domain on Startup** option if you want to select a domain to open when Policy Manager is launched.
6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## SNMP Options

Use the [SNMP Options view](#) to specify SNMP polling parameters for the Policy Manager server and client.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Policy Manager folder and select SNMP Options. The right-panel SNMP Options view is displayed.
3. Under **Server SNMP**, specify SNMP polling parameters for the Policy Manager server. These settings apply to all users.
  - **SNMP Retries** - The number of times the server will attempt to contact a device after the first attempt fails. The default setting is 3 retries, which means that the server retries a timed-out request three times, making a total of four attempts to contact a device.
  - **SNMP Timeout** - The amount of time (in seconds) that the server waits before re-trying to contact a device.
4. In the **Enforce/Verify** section, select the "Force read of policy rules table" option to change how the Policy Manager verify operation is performed. During the verify operation, Policy Manager uses the "Last Changed" attribute on the device to determine if any rules have changed. Selecting the "Force read of policy rules table" option causes Policy Manager to

perform the verify operation using the rules table instead of the attribute. This can cause the verify operation to take longer to perform. Normally this option is not selected and should only be enabled for specific customer deployments as instructed by Extreme Networks Support.

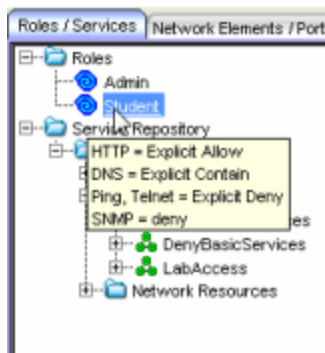
5. Under **Client SNMP**, specify SNMP polling parameters for the Policy Manager client. These settings apply to the current user.
  - **SNMP Retries** - The number of times the client will attempt to contact a device after the first attempt fails. The default setting is 3 retries, which means that the client retries a timed-out request three times, making a total of four attempts to contact a device.
  - **SNMP Timeout** - The amount of time (in seconds) that the client waits before re-trying to contact a device.
6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Tab Configuration

Use the [Tab Configuration view](#) to specify the top-level tab organization for your domains. By default, all domains will use the configuration defined here. However, it is possible to override these setting on a per-domain basis using the View > Domain Tab Configuration menu. Any new domain you create will use the settings specified here. These settings apply 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 Policy Manager folder and select Tab Configuration. The right-panel Tab Configuration view is displayed.
3. Use the **Domain Default Tab Configuration** drop-down list to select the tab configuration you would like to use in your domains:
  - **Consolidated Tab Configuration (Recommended)** - In this configuration, there are two top-level tabs: Roles/Services and Network Elements/Port Groups. Access Control and Class of Service trees are presented in external Configuration windows accessed from the Edit menu.
  - **Classic Tab Configuration** - This configuration uses six top-level tabs, one for each Policy Manager tree: Roles, Services, Access Control, Classes of Service, Network Elements, and Port Groups. This is similar to the configuration used in Policy Manager prior to version 4.0.

- Custom Tab Configuration - This configuration allows you to define which tab the different Policy Manager trees will be organized under. For Access Control and Classes of Service trees, you can also select to display the tree in a Configuration View (an external window) accessed from the Edit menu.
4. Use the **Select Tree at Startup** drop-down list to specify the tree that will be selected in the left-panel when you start Policy Manager.
  5. Select **Show Description fields as tooltips in trees** if you want a description of each node in a tree to be displayed (if available) in a tooltip when the cursor hovers over the node. In the example below, you can see that a description of the Student role is displayed when the cursor hovers over the Student node in the tree.



6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

## Welcome View

Use the [Welcome View option](#) to display or hide the Welcome tab that is displayed when you first open Policy Manager. 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 Policy Manager folder and select Welcome View. The right-panel Welcome View option is displayed.
3. Select whether to display or hide the Welcome tab when Policy Manager is first opened.
4. Click **OK** to set the option and close the window. Click **Apply** to set the option and leave the window open.

## Wireshark

Use the [Wireshark view](#) to specify the location of the Wireshark executable so that it can be used by Policy Manager to display rule color filters. For more information on using Wireshark in Policy Manager, see [How to Use Wireshark to Analyze a Role's Behavior](#). 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 Policy Manager folder and select Wireshark. The right-panel Wireshark view is displayed.
3. Enter the location of the Wireshark executable or use the **Browse** button to navigate to the executable file.
4. Click **OK** to set the option and close the window. Click **Apply** to set the option and leave the window open.

---

### Related Information

For information on related windows:

- [Options Window, Policy Manager Options](#)

## How to Use Wireshark® to Analyze a Role's Behavior

---

This Help topic describes how to launch Wireshark® against a Policy Manager role, providing a quick, visual representation of how the role would handle network traffic. Wireshark can be launched against either a pre-existing data capture (.pcap file) or a live data capture (local and remote), and uses color filters to color the traffic based on the actions configured for the role's rules or the role's default action. This allows you to see how the traffic would have been handled had the role been applied to the end-system at the time of the traffic capture.

You can create color filters for the following action types:

- Access Control
- Class of Service (802.1p Priority)
- System Log
- Audit Trap
- Disable Port
- Traffic Mirror

Because Wireshark is launched against a role's current configuration, and not the current configuration on a network device, you do not need to configure any network device in order to see how the role will handle traffic. This makes Wireshark very useful when planning your network roles, by demonstrating the benefits of the role before enforcing the role to your network devices.

In addition, Policy Manager provides the ability to simultaneously launch multiple instances of Wireshark, allowing:

- Side-by-side comparison of two roles against the same captured data.
- Side-by-side comparison of the same role with different rule sets against the same captured data.

This Help topic assumes that you have installed Wireshark and are familiar with its usage. Before using Wireshark with Policy Manager, make sure that the location of the Wireshark executable is set correctly in the Policy Manager Wireshark option (Tools > Options > Policy Manager > Wireshark). For information on installing and using Wireshark, go to [www.wireshark.org](http://www.wireshark.org).

Instructions on:

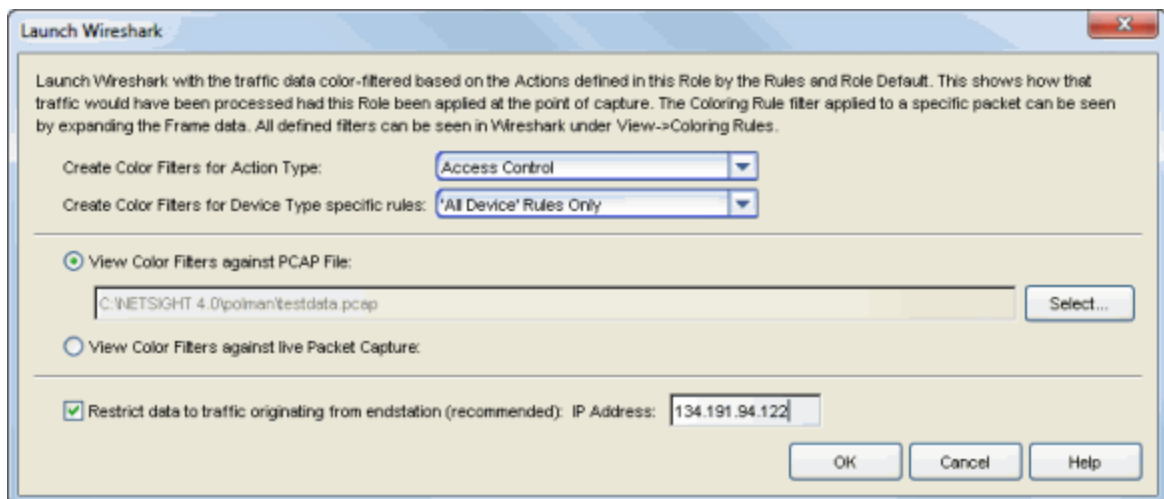
- [Launching Wireshark](#)
  - [Launching Against a Data Capture](#)
  - [Launching Against Live Local Traffic](#)
  - [Launching Against Live Remote Traffic](#)
- [Viewing Wireshark](#)
  - [Wireshark Color Filter Scheme](#)
  - [Determining Rule Hit](#)
  - [Viewing Color Filters](#)

## Launching Wireshark

The steps for launching Wireshark vary slightly depending on whether you will be launching Wireshark against a data capture file, live local traffic, or live remote traffic. Each method for launching Wireshark is described below.

### *Launching Against a Data Capture*

1. In the left-panel Roles tab, right-click on the role you want to view with Wireshark, and select the **Launch Wireshark with Rule Color Filters** option from the menu. The Launch Wireshark window opens.



2. Select the **Action Type** you would like color filters created for. Wireshark will color-filter the traffic data based on how that specific action type is defined in the role by the rules and the role default actions.



3. If you want to **create color filters only for certain device type specific rules**, use the drop-down list to select the device type. Otherwise, select "All Device" Rules Only.
4. Select the **View Color Filters against PCAP File** radio button, and use the **Select** button to navigate to the .pcap file you want to use.
5. Select the **Restrict data to traffic originating from endstation** checkbox. This option will filter out return and broadcast traffic, allowing Wireshark to accurately reflect only the traffic that would be filtered by the role being applied to a user. Enter a valid IP address or hostname for the endstation, or enter "localhost." Click **OK**.
6. Wireshark opens, displaying the data. Go to [Viewing Wireshark](#) for information on viewing the data.

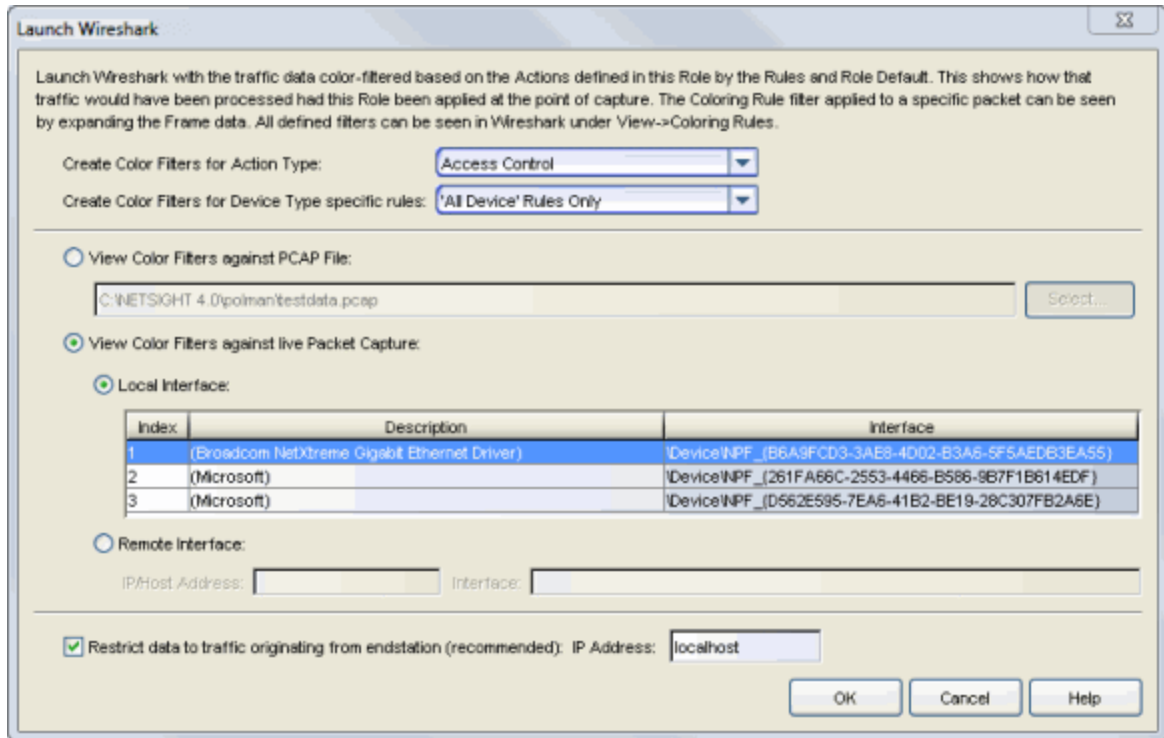
---

**NOTE:** If no data appears when Wireshark opens, the endstation IP address entered in step 4 does not match the source IP of any traffic in the .pcap file.

---

### *Launching Against Live Local Traffic*

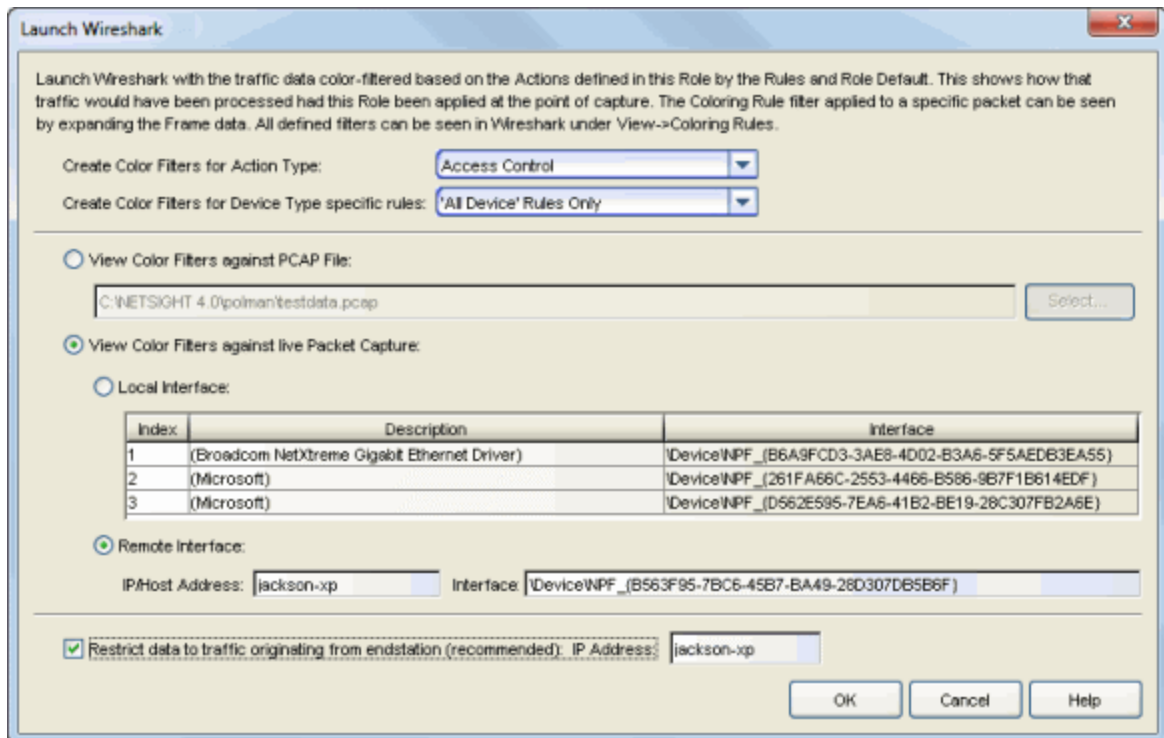
1. In the left-panel Roles tab, right-click on the role you want to view with Wireshark, and select the **Launch Wireshark with Rule Color Filters** option from the menu. The Launch Wireshark window opens.



2. Select the **Action Type** you would like color filters created for. Wireshark will color-filter the traffic data based on how that specific action type is defined in the role by the rules and the role default actions.
3. If you want to **create color filters only for certain device type specific rules**, use the drop-down list to select the device type. Otherwise, select "All Device" Rules Only.
4. Select the **View Color Filters against live Packet Capture** radio button, and then the **Local Interface** radio button. Select the appropriate interface in the table. If multiple interfaces are displayed, it is important to select the one from which traffic is being sent.
5. Select the checkbox **Restrict data to traffic originating from endstation**. This option will filter out return and broadcast traffic, allowing Wireshark to accurately reflect only the traffic that would be filtered by the role being applied to a user. Verify that the endstation's IP address, hostname, or "localhost" (the default) is entered in the field. See the [Note](#) below if you are configuring Wireshark in a port mirroring scenario. Click **OK**.
6. Wireshark opens, displaying the data. Go to [Viewing Wireshark](#) for information on viewing the data.

## Launching Against Live Remote Traffic

1. In the left-panel Roles tab, right-click on the role you want to view with Wireshark, and select the **Launch Wireshark with Rule Color Filters** option from the menu. The Launch Wireshark window opens.



2. Select the **Action Type** you would like color filters created for. Wireshark will color-filter the traffic data based on how that specific action type is defined in the role by the rules and the role default actions.
3. If you want to **create color filters only for certain device type specific rules**, use the drop-down list to select the device type. Otherwise, select "All Device" Rules Only.
4. Select the **View Color Filters against live Packet Capture** radio button, and then the **Remote Interface** radio button.
5. Enter the proper values to capture data on a remote endstation. You must have a remote pcap daemon (e.g. rpcapd) running on the specified endstation, with NULL authentication allowed (-n flag).
  - a. Enter the endstation's IP address or hostname.
  - b. Enter the interface value, which should look similar to:  
`\Device\NPF_{F6E3014E-83EC-4EB4-994C-1D5F3963B12A}`  
 There are a couple of ways you can determine the interface value:

- If Wireshark is installed on the remote endstation, you can see the interface values in the Wireshark application if it is launched. Additionally, running Wireshark from the endstation command line with the "-D" flag will output the interface values.
  - The Nmap Application ([www.nmap.org](http://www.nmap.org)) is another mechanism for detecting the interface value. The interface string for the remote interface can be determined by running `nmap --iflist` on the remote endstation.
6. Select the checkbox **Restrict data to traffic originating from endstation**. This option will filter out return and broadcast traffic allowing Wireshark to accurately reflect only the traffic that would be filtered by the role being applied to a user. Verify that the endstation's IP address or hostname is entered in the field. See the following [Note](#) if you are configuring Wireshark in a port mirroring scenario. Click **OK**.
  7. Wireshark opens, displaying the data. Go to [Viewing Wireshark](#) for information on viewing the data.

---

**NOTE:** If you have set up a traffic mirror on a role that is already deployed to an endstation, and are using Wireshark to setup a local or remote capture, the endstation filter should specify the endstation that is the **source** of the port mirror (the one already assigned a role), rather than the endstation capturing the traffic. This would show what traffic is currently being permitted by the switch from that user.

---

## Viewing Wireshark

Once you have launched Wireshark using the instructions in the previous section, the Wireshark window opens displaying the traffic data. The data is colored according to the rules defined by the role, and the role default actions.

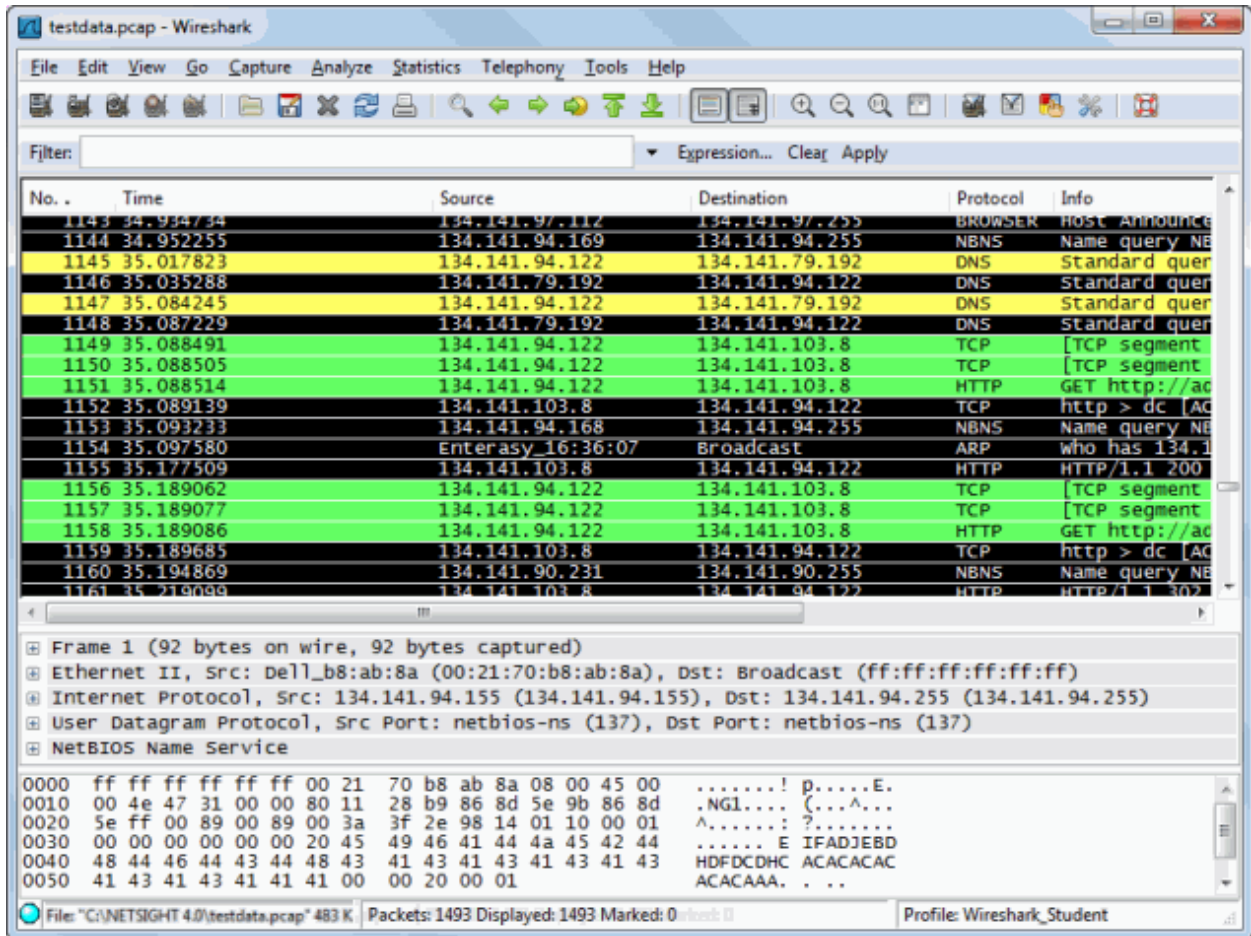
### *Wireshark Color Filter Scheme*

The Wireshark color filter scheme that is used varies according to the selected Action Type:

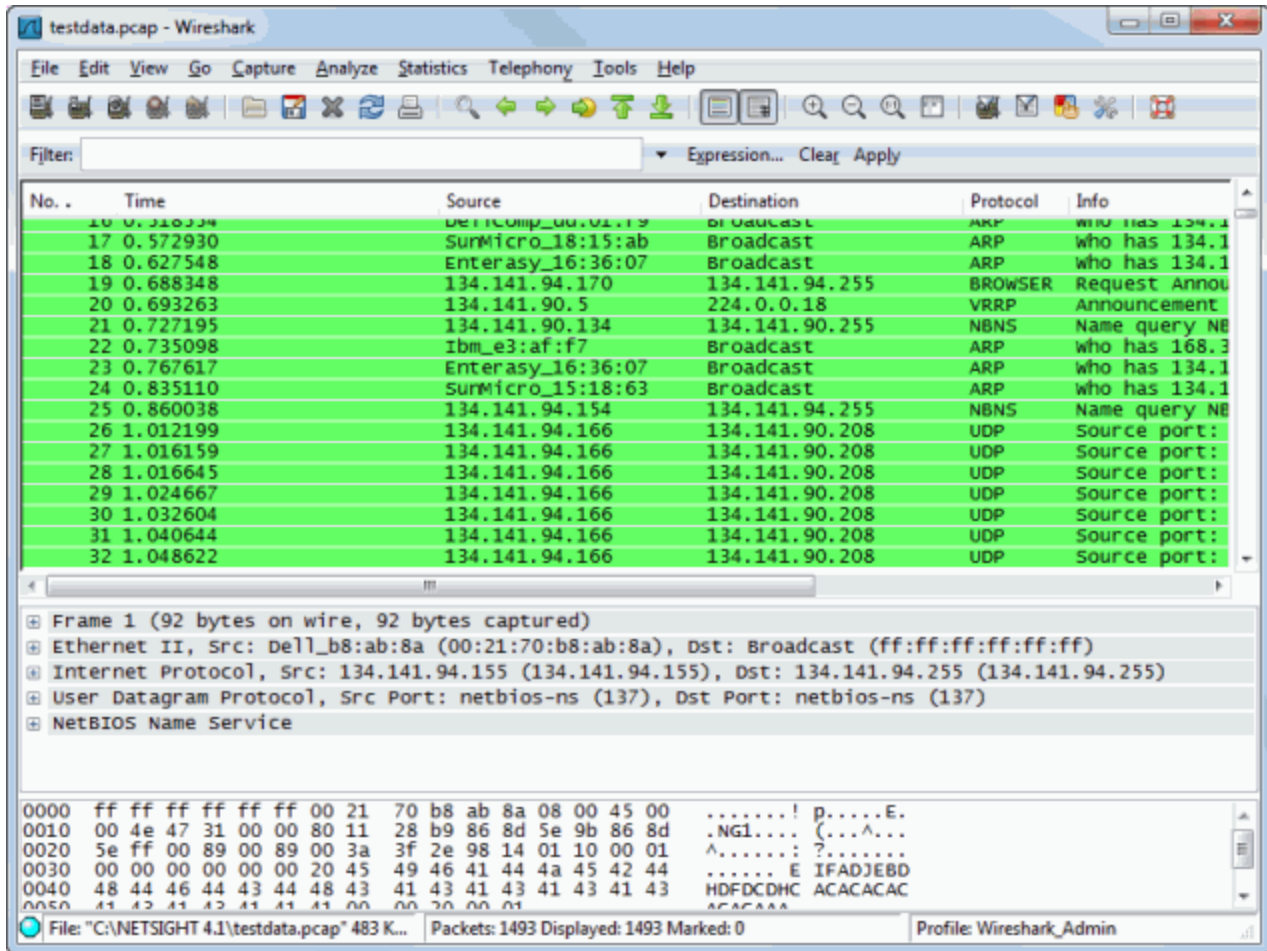
- **Access Control**
  - Discarded traffic is colored black
    - Discard Rule = pink text
    - Role Default Discard = white text

- Permitted traffic is colored green
  - Permit Rule = bright green
  - Role Default Permit = pale green
- Contained to a VLAN traffic is colored yellow
  - Contain Rule = bright yellow
  - Role Default Contain = pale yellow
- **Class of Service (802.1p Priority)** Each of the 802.1p Priorities (0-7) are assigned a different color filter ranging from bright green to bright red for rules and from pale green to pale red for role defaults. For rules using a user-defined class of service with no priority, the color filter is blue.
- **System Log**
  - Prohibited Rule = yellow
  - Enabled Rule = bright green
  - Role Default = pale green
- **Audit Trap**
  - Prohibited Rule = yellow
  - Enabled Rule = bright green
  - Role Default = pale green
- **Disable Port**
  - Prohibited Rule = yellow
  - Enabled Rule = bright red
  - Role Default = pale red
- **Traffic Mirror**
  - Prohibited Rule = yellow
  - Enabled Rule = bright green
  - Role Default = pale green

The following two examples display Wireshark launched against a data capture file using two different roles: Student and Admin. The first example shows how the Student role contains DNS traffic (pale yellow), denies certain traffic (black), and permits Web traffic (bright green).

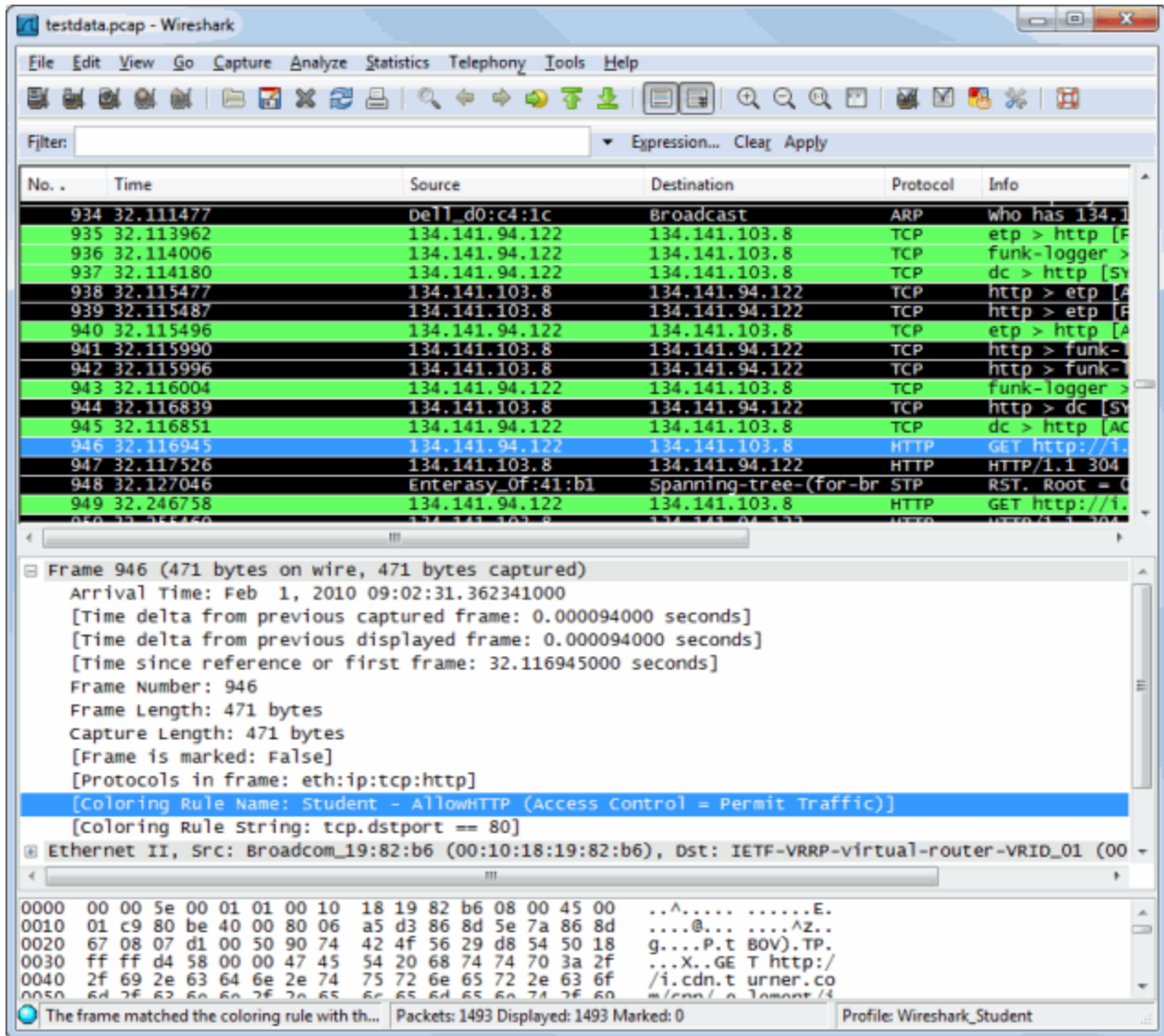


This second example shows how the Admin role allows all traffic (bright green) according to the role's permit rules.



### Determining Rule Hit

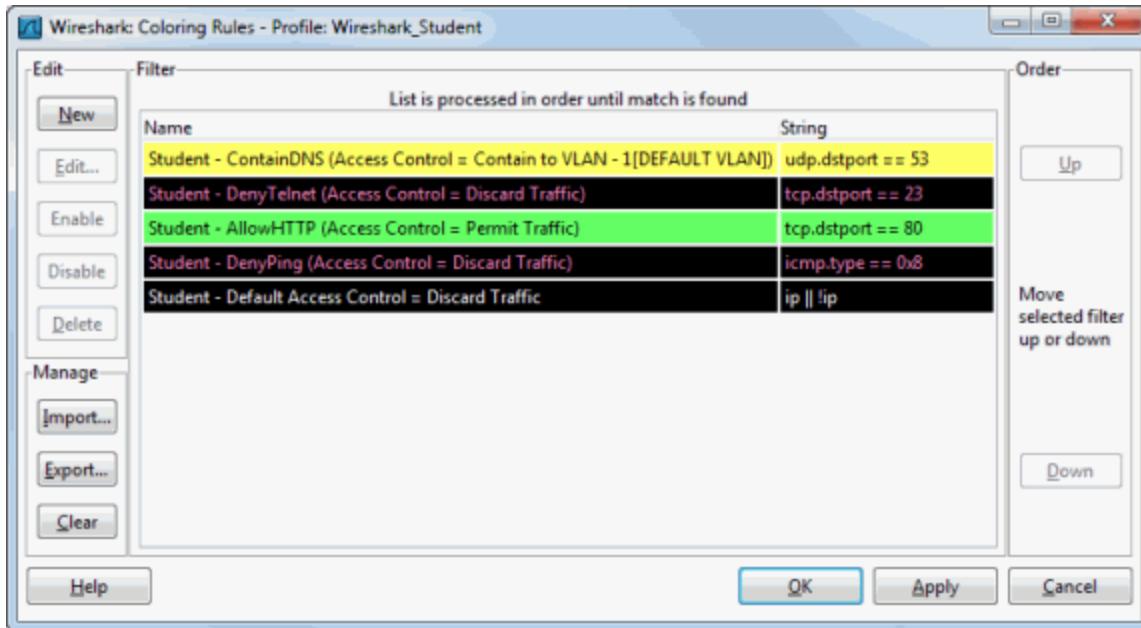
You can determine the specific rule that each packet hit by selecting the packet in the table, and then looking in the Coloring Rule Name field in the Frame packet data at the bottom of the screen. The example below shows that the "AllowHTTP" rule in the Student role caused the selected packet to be permitted (bright green).



### Viewing Color Filters

You can view all the color filters used for a role by selecting **View > Coloring Rules** from the Wireshark window. Refer to the Wireshark documentation for information on using the Coloring Rules window.





## Related Information

For information on related tabs:

- [General Tab \(Rule\)](#)
- [General Tab \(Role\)](#)

## Policy Classification Rules Window

---

The Policy Classification Rules window provides a way to view all of the Policy Manager rules that exist in either the currently active domain or all domains, and displays information about each rule. Access this window by selecting one of the following options from the menu bar.

- **View > Policy Classification Rules** - to view all the rules that exist in the currently active domain
- **Domain > Show All Rules for All Domains** - to view all the rules that exist in all your domains

Information on the following Policy Classification Rules views:

- [Rules for the Current Domain](#)
- [Rules for All Domains](#)

### Rules for the Current Domain


This window lets you view all the Policy Manager rules that exist in the currently active domain. To access the window, select **View > Policy Classification Rules** from the menu bar. Clicking on a column heading sorts the column. Use the buttons at the bottom of the window to export or print the table.

Name of Rule	Rule Status	Rule Type	Traf Desc Type	Traf Desc
Discard IP Protocol Type ICMP	Enabled	All Devices	IP Protocol Type	ICMP
Discard TCP Bil 22 - SSH	Enabled	All Devices	IP TCP Port Bilateral	SSH
Discard TCP Bil 23 - Telnet	Enabled	All Devices	IP TCP Port Bilateral	Telnet
Discard TCP Src 20 - FTP Data	Enabled	All Devices	IP TCP Port Source	FTP Data
Discard TCP Src 21 - FTP	Enabled	All Devices	IP TCP Port Source	FTP
Discard TCP Src 25 SMTP	Enabled	All Devices	IP TCP Port Source	SMTP
Discard TCP Src 53 - DNS zo...	Enabled	All Devices	IP TCP Port Source	DNS
Discard TCP Src 80 - HTTP	Enabled	All Devices	IP TCP Port Source	HTTP
Discard TCP Src 443 - SSL	Enabled	All Devices	IP TCP Port Source	HTTPS
Discard UDP Bil 69 - TFTP	Enabled	All Devices	IP UDP Port Bilateral	TFTP
Discard UDP Bil 161 - SNMP	Enabled	All Devices	IP UDP Port Bilateral	SNMP
Discard UDP Bil 162 - TRAPS	Enabled	All Devices	IP UDP Port Bilateral	162
Discard UDP Src 53 - DNS Im	Enabled	All Devices	IP UDP Port Source	DNS


### Name of Rule

The name assigned to the rule. If a rule has been applied to a specific device type (see [Rule Type](#)), that device type will precede the rule name, in brackets.

### Rule Status

The status of the rule: Enabled or Disabled. If a rule is disabled, it is unavailable for use by the service with which it is associated, but can still be copied to other services and enabled. Disabling a rule is an alternative to deleting and recreating it. The rule icon in the left panel displays a red X  if the rule is disabled. For more information, see [Disabling/Enabling a Rule](#).

### Rule Type

The rule type selected when the rule was created. Rule type specifies the type of device to which the rule is applied when enforced, or all devices. If the rule is device-specific, the rule icon displays a small switch . See [Rule Type](#) for more information.

### Traf Desc Type

The traffic description (classification type) defined for the rule. The traffic description identifies the type of traffic to which the rule will pertain. See [Classification Types and their Parameters](#) for a description of classification layers and types.

**Traf Desc Value**

Each traffic description (classification type) requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information.

**Traf Desc Mask**

The mask for the rule's classification type, if applicable.

**Access Control**

The access control (VLAN assignment) defined for the rule. The rule's access control specifies whether to:

- Permit Traffic - traffic will be forwarded with the port's assigned VID
- Deny Traffic - traffic will be denied altogether
- Contain to VLAN - traffic is contained to a specified VLAN

**CoS**

The class of service associated with the rule. A class of service includes an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, drop precedence, rate limits, and transmit queue configuration. See [Getting Started with Class of Service](#) and [How to Create a Class of Service](#) for more information.

**Sys Log**

Indicates whether a syslog message is generated when the rule is used, as set in the [General tab](#) for the rule.

**Trap**

Indicates whether an audit trap is generated when the rule is used, as set in the [General tab](#) for the rule.

**Disable Port**

Indicates whether any port reported as using this rule will be disabled, as set in the [General tab](#) for the rule.

**Service Name**

Lists any services the rule belongs to.

**Service Group**

Lists any service groups the rule belongs to.

**In Role**

Lists any roles the rule belongs to.

## Rules for All Domains

This window lets you view all the rules that exist in all your domains. To access the window, select **Domain > Show All Rules for All Domains** from the menu bar. Clicking on a column heading sorts the column. Use the buttons at the bottom of the window to export or print the table.

Domain	In Role	Name of Rule	Rule Status	Rule Type
Default Policy Domain	Guest Access	[SecureStack C2/B2] Deny UDP	Enabled	SecureStack C2/B2
Default Policy Domain	Guest Access	[SecureStack C2/B2] Permit Bootps	Enabled	SecureStack C2/B2
Default Policy Domain	Guest Access	[SecureStack C2/B2] Permit DNS	Enabled	SecureStack C2/B2
Default Policy Domain	Guest Access	[SecureStack C2/B2] Permit HTTP	Enabled	SecureStack C2/B2
Default Policy Domain	Guest Access	[SecureStack C2/B2] Permit HTTPS	Enabled	SecureStack C2/B2
Default Policy Domain	Guest Access	[SecureStack C2/B2] Permit PPTP	Enabled	SecureStack C2/B2
Dormitory	Enterprise Access	Discard AppleTalk	Enabled	All Devices
Dormitory	Enterprise Access	Discard AppleTalk ARPs	Enabled	All Devices
Dormitory	Enterprise Access	Discard Banyan Vines	Enabled	All Devices
Dormitory	Enterprise Access	Discard DSAP/SSAP IPX	Enabled	All Devices
Dormitory	Enterprise Access	Discard DSAP/SSAP NetBIOS	Enabled	All Devices
Dormitory	Enterprise Access	Discard DSAP/SSAP SNA	Enabled	All Devices
Dormitory	Enterprise Access	Discard Decnet Phase 4	Enabled	All Devices
Dormitory	Enterprise Access	Discard IP Protocol Type OSPF	Enabled	All Devices
Dormitory	Enterprise Access	Discard IPX RIP	Enabled	All Devices

### Domain

The name of the domain the rule exists in.


### In Role

Lists any roles the rule belongs to.


### Name of Rule

The name assigned to the rule. If a rule has been applied to a specific device type (see [Rule Type](#)), that device type will precede the rule name, in brackets.

### Rule Status

The status of the rule: Enabled or Disabled. If a rule is disabled, it is unavailable for use by the service with which it is associated, but can still be copied to other services and enabled. Disabling a rule is an alternative to deleting and recreating it. The rule icon displays a red X  if the rule is disabled. For more information, see [Disabling/Enabling a Rule](#).

**Rule Type**

The rule type selected when the rule was created. Rule type specifies the type of device to which the rule is applied when enforced, or all devices. If the rule is device-specific, the rule icon displays a small switch . See [Rule Type](#) for more information.

**Traf Desc Type**

The traffic description (classification type) defined for the rule. The traffic description identifies the type of traffic to which the rule will pertain. See [Classification Types and their Parameters](#) for a description of classification layers and types.

**Traf Desc Value**

Each traffic description (classification type) requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information.

**Traf Desc Mask**

The mask for the rule's classification type, if applicable.

**Access Control**

The access control (VLAN assignment) defined for the rule. The rule's access control specifies whether to:

- Permit Traffic - traffic will be forwarded with the port's assigned VID
- Deny Traffic - traffic will be denied altogether
- Contain to VLAN - traffic is contained to a specified VLAN

**CoS**

The class of service associated with the rule. A class of service includes an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, drop precedence, rate limits, and transmit queue configuration. See [Getting Started with Class of Service](#) and [How to Create a Class of Service](#) for more information.

**Sys Log**

Indicates whether a syslog message is generated when the rule is used, as set in the [General tab](#) for the rule.

**Audit Trap**

Indicates whether an audit trap is generated when the rule is used, as set in the [General tab](#) for the rule.

**Disable Port**

Indicates whether any port reported as using this rule will be disabled, as set in the [General tab](#) for the rule.

**Service Name**

Lists any services the rule belongs to.

**Service Group**

Lists any service groups the rule belongs to.

**Event Log Button**

Opens the [event log](#).

**Export Table Button**

Exports the information in this window to an HTML file. Clicking Export Table opens a Save as Web Page window where you can name your exported file, and navigate to a folder/directory where you want to place the file.

**Update View Button**

Updates the information in the window.

**Print Button**

Prints the information in the window.

---

**Related Information**

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)
- [How to Create a Service](#)

For information on related windows:

- [General Tab \(Rule\)](#)

## Policy Manager Right-Panel Tabs

---

The Policy Manager main window is divided into two panels: a left panel and a right panel. The Right-Panel Tabs Help section contains Help topics describing the tabs and their field definitions.

The right panel displays different tabs and information depending on the item selected in the left-panel tree. Help topics for right-panel tabs are named in a manner to reflect this. For example, the help topic named Details View Tab (Device Group), provides information on the right-panel Details View tab when a device group is selected in the left-panel tree.



## Anti-Spoofing Tab (Device)

---

The device Anti-Spoofing tab allows you to configure the anti-spoofing settings and violation actions for the selected device. Anti-spoofing must be configured and enabled on the device in order for individual port anti-spoofing settings to take effect. For more information about the anti-spoofing feature, see [How to Configure Anti-Spoofing](#).

To access this tab, select a device on the left panel's Network Elements tab, then click the Anti-Spoofing tab in the right panel.

There are three sub-tabs that provide different anti-spoofing configuration information.

- [Device Configuration](#)
- [Port Configuration](#)
- [Station Bindings](#)

### Device Configuration

This tab provides access to all device-level anti-spoofing configuration. The General Settings section allows you to enable or disable anti-spoofing, audit traps, and duplicate IP checking. The Violation Actions section lets you configure the actions to impose on users that violate the station bindings that are created through anti-spoofing.

Details View | Ports | General | Role/Rule | Authentication | Port Usage | RADIUS | **Anti-Spoofing** | MAC Locking | Rule Usage

Device Configuration | Port Configuration | Station Bindings

**General Settings**

Anti-Spoofing: Enabled

Audit Traps: Disabled

Audit Trap Interval (sec): 60

Duplicate IP Checking: Enabled

Apply

**Violation Actions**

Edge Ports (4 Ports) | Uplink Ports (2 Ports) | Static Ports (2 Ports)

Port Class Index: 1

Port Class Name: Edge Ports

Counter Timeout (sec): 600

Note: Quarantine Role actions require Quarantine Auth status be enabled for device & port(s)

Index	Value	Actions	Ports
1	1	Syslog	[12.22.88.141] Port ge.1.5
2	2	Audit Trap	[12.22.88.141] Port ge.1.12
3	3	Audit Trap	[12.22.88.141] Port ge.1.13
4	4	Quarantine Role (Quarantine)	[12.22.88.141] Port ge.1.18
5	--	None	
6	--	None	

Edit Action(s) | Remove Action(s) | Add/Remove Ports | Port Properties... | Apply

## General Settings

### Anti-Spoofing

Use the drop-down menu to enable or disable anti-spoofing for the device.

### Auto Traps

Use the drop-down menu to enable or disable audit traps for the device. This must be enabled if you have configured an audit trap as a threshold action, in order for the trap to be sent.

### Audit Trap Interval (sec)

The number of seconds to wait before generating another audit trap for the same user. For example, in the case of a user who continually changes IP addresses, if you have multiple thresholds set to trigger audit traps, this interval prevents a large number of audit traps from being sent in a very short time. The default interval is 60 seconds. A value of zero (0) indicates that no audit traps related to anti-spoofing will be suppressed.

## Duplicate IP Checking

Use the drop-down menu to enable or disable duplicate IP checking on the device. This functionality logs duplicate IP addresses when they are bound to different MAC addresses, using syslog messages and audit traps. Read more about duplicate IP checking in [How to Configure Anti-Spoofing](#).

## Apply

Saves any change you made to the General settings.

## *Violation Actions*

This section is where you define the threshold values and resulting actions that will be used when MAC-to-IP address binding violations occur on the device.

Thresholds are the number of violations that must occur on a single MAC-to-IP address binding before an action is performed. Each threshold can be assigned one or more of the following actions: sending a syslog message, sending an audit trap, or applying a quarantine policy.

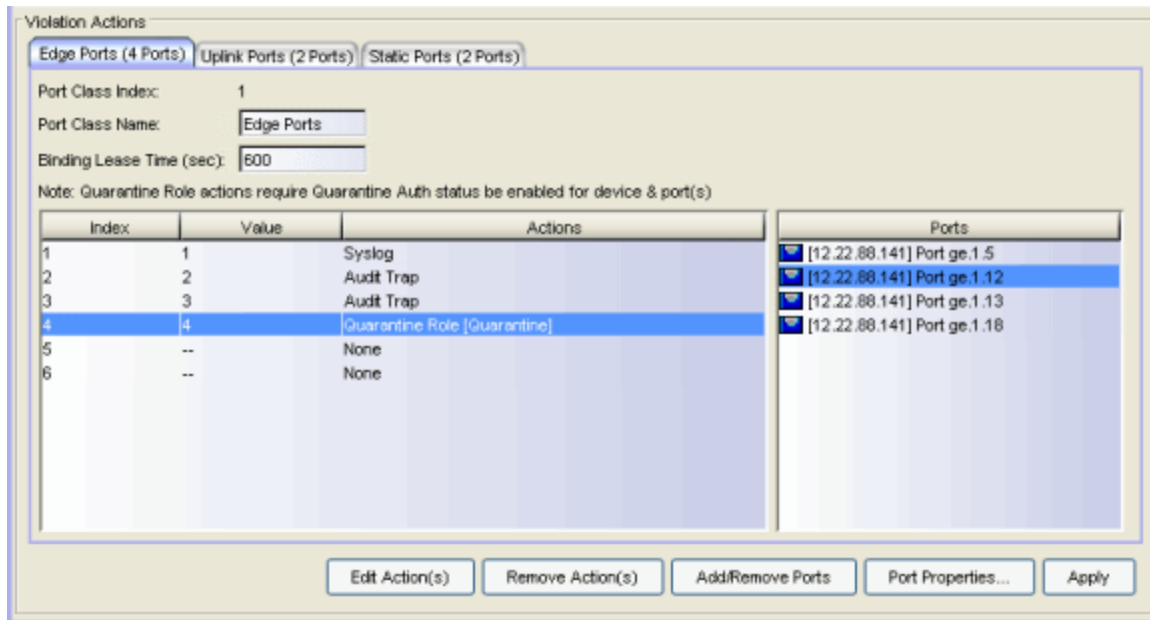
You can define thresholds and actions for up to three different port classes per device. Port classes allow you to assign the ports on a device into different groups depending on port type.

For example, you might configure a port class for your edge ports and another port class for your uplink ports, and define different thresholds and actions for each port class. You might also want to configure a port class for ports with statically assigned addresses, allowing for a stricter threshold configuration. Another option is to configure port classes for ports that are using different methods to create MAC-to-IP bindings, such as DHCP snooping ports in one class and IP source guard ports in another class.

Up to six thresholds can be configured per port class. Typically, thresholds values are set to a low number. For example, you could configure a threshold value of 2 to trigger a syslog message to alert administrators of a binding violation. You could configure another threshold value of 5 to assign a quarantine role to a user. That way, if a user continues to violate a binding, you can restrict their access until the cause of the violation can be determined.

To create or edit a threshold and action, select a port class and then select an action index number in the table and click the **Edit Action(s)** button or double-click the row. The Edit Action window opens where you can configure the threshold value and action. If you assign a quarantine action, you must associate a valid quarantine policy with the quarantine action. For more information, refer to [How to Create a Quarantine Role](#).

For each port class, you must assign the ports that will be part of the class. A port can be assigned to only one class. Use the **Add/Remove Ports** button to add or remove ports to or from the class. In addition, you can select a port and click the **Port Properties** button to open the Port Properties window where you can configure the port-level anti-spoofing options for the selected port.



### Port Class Index

Up to three port classes can be configured on the switch. This index number shows which port class is being configured.

### Port Class name

Use this field to set a name for the port class, for example, Edge Ports.

### Binding Lease Time (sec)

The number of seconds a binding will exist before being removed by the device.

### Edit Actions

Select an action and click this button to open the Edit Actions window, where you can configure the threshold value and action.

### Remove Actions

This button removes any selected actions.

### Add/Remove Ports

Use this button to add or remove ports from this port class.

## Port Properties

Select a port and click this button to open the [Port Properties window](#) where you can configure the port-level anti-spoofing options for the selected port. You can also configure port-level anti-spoofing options in the Port Configuration sub-tab.

## Apply

Saves any change you made to the Violation Actions settings.

## Port Configuration

This tab displays the port-level anti-spoofing settings for each port on the device. You can change port settings for one or more ports by multi-selecting ports and using the right-click menu. See below for a description of each column in the table.

Right-click one or more rows to change Anti-Spoofing settings.

Port	Port Type	AS Port Type	DHCP Snooping	DHCP MAC Verify	Dynamic ARP Inspection	IP Source Guard	Untrusted D
[10.20.88.8] Port ge.1.1	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.2	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.3	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.4	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.5	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.6	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.7	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.8	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.9	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.10	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.11	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.12	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.13	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.14	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.15	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.16	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.17	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.18	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.19	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.20	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.21	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.22	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.23	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.24	CDP	Trusted	Enabled	Disabled	Enabled	Enabled	0
[10.20.88.8] Port ge.1.25	Access	Untrusted	Enabled	Disabled	Enabled	Enabled	0

## Port

Displays the port name, constructed of the name or IP address of the device and either the port index number or the port interface name.

## Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

## AS Port Type

The DHCP snooping port type configured for the port. Port type determines anti-spoofing behavior:

**Trusted** - DHCP server traffic is accepted and used to create bindings in the MAC-to-IP address binding table. Typically, only a port that is connected to a DHCP server would be set to trusted.

**Bypass** - Snooping of DHCP server traffic does not take place on the port. Typically, uplink ports out to the network would be set to bypass, as traffic would not be originating from that port.

**Untrusted** - The untrusted server counter is incremented when DHCP server traffic (DHCP ACK) is detected on the port, and the packets are dropped. DHCP RELEASE and DECLINE messages, sent by a client to free its IP address for use by another, are dropped if they are for a MAC address in the binding table that is on another port. If [DHCP MAC Verify](#) is enabled and the source MAC address does not match the Client Host Address in the DHCP payload (CHADDR), the packets are dropped. Typically, all edge ports with users would be set to untrusted.

## DHCP Snooping

Whether [DHCP Snooping](#) is enabled or disabled on the port.

## DHCP MAC Verify

Whether [DHCP MAC Verify](#) is enabled or disabled on the port.

## Dynamic ARP Inspection

Whether [Dynamic ARP Inspection](#) is enabled or disabled on the port. When set to inspection only, Dynamic ARP inspection will occur, but will not be used to create bindings.

## IP Source Guard

Whether [IP Source Guard](#) is enabled or disabled on the port. When set to inspection only, IP Source Guard will occur, but will not be used to create bindings.

## Untrusted DHCP Packet Count

The number of DHCP server packets received on this port. This counter will only increment when the Port Type is set to untrusted.

## Station Bindings

The Station Bindings table displays the current active bindings for the device set up through anti-spoofing. These bindings are the valid MAC/IP/Port

associations detected on trusted ports from the various anti-spoofing methods such as DHCP requests. This tab also provides the ability to reset violation counters and clear bindings from the table. You must click the **Retrieve** button to display this information.

MAC Address	IP Address	Hostname	Port	IP Change Count	Binding Type	Duration (sec)	Lease Time (sec)
00:1F:45:47:4B:F4	12.22.88.136		[12.22.88.1] Port ge.1.9		IP	491	600
00:11:88:BD:CC:36	12.22.88.138		[12.22.88.1] Port ge.1.10		IP	480	600
00:11:88:FD:91:40	12.22.88.141		[12.22.88.1] Port ge.1.11		IP	467	600
00:11:88:A9:19:A0	12.22.88.134		[12.22.88.1] Port ge.1.12		IP	79	600
00:1F:45:47:76:34	12.22.88.135		[12.22.88.1] Port ge.1.13		IP	480	600
00:1F:45:7A:1B:CC	12.22.88.137		[12.22.88.1] Port ge.1.15		IP	491	600
00:11:88:A9:7D:20	12.22.88.131		[12.22.88.1] Port ge.1.16		ARP	474	600
00:11:88:16:8B:01	12.22.80.126		[12.22.88.1] Port ge.1.17		ARP	467	600
00:00:12:10:09:08	12.22.88.169		[12.22.88.1] Port ge.1.18		IP	209	600
00:11:88:72:2C:00	12.22.88.132		[12.22.88.1] Port ge.1.19		ARP	408	600
00:11:88:B9:98:9E	12.22.80.161		[12.22.88.1] Port ge.1.21		IP	366	600
00:11:88:BA:96:50	12.22.82.131		[12.22.88.1] Port ge.1.21		IP	475	600
00:0C:29:B7:A6:03	12.22.80.61		[12.22.88.1] Port ge.1.21		IP	496	600
00:11:88:BA:96:20	12.22.80.171		[12.22.88.1] Port ge.1.21		IP	379	600
00:11:88:FA:9C:09	12.22.80.16		[12.22.88.1] Port ge.1.21		IP	440	600
00:15:C5:58:13:9E	12.22.80.150		[12.22.88.1] Port ge.1.21	120	DHCP	13	60
00:10:18:27:DE:C3	12.22.80.2		[12.22.88.1] Port ge.1.21		IP	493	600
00:11:88:E8:08:68	12.22.85.10		[12.22.88.1] Port ge.1.21		IP	477	600
00:1F:45:08:33:00	12.22.80.12		[12.22.88.1] Port ge.1.21		ARP	439	600
00:11:88:FB:CB:D2	12.22.80.88		[12.22.88.1] Port ge.1.21		IP	497	600
00:11:88:B7:40:86	12.22.80.170		[12.22.88.1] Port ge.1.21		IP	499	600
00:11:88:E4:8C:95	12.22.85.11		[12.22.88.1] Port ge.1.21		IP	440	600
00:1F:45:08:33:1F	12.22.86.27		[12.22.88.1] Port ge.1.21	13	IP	481	600
00:11:88:3A:33:F4	12.22.82.132		[12.22.88.1] Port ge.1.21		ARP	346	600
00:02:B3:EC:F7:84	12.22.80.48		[12.22.88.1] Port ge.1.23		IP	495	600
20:B3:99:5E:DB:94	12.22.80.130		[12.22.88.1] Port ge.1.23		IP	437	600

### MAC Address

The MAC address of the binding.

### IP Address

The IP address of the binding.

### Hostname

An administratively-assigned hostname for the device. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Anti-Spoofing Station Binding views using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

### Port

The port that this binding currently resides on.

### IP Change Count

The number of times the IP address has changed for this binding.

**Binding Type**

Indicates which binding type (DHCP, ARP, or IP inspection) was used to create the entry.

**Duration (sec)**

The amount of time, in seconds, that this binding has been operational for.

**Lease Time (sec)**

The amount of time, in seconds, that this binding will be operational before being destroyed. A value of zero (0) indicates that this binding will not expire.

**Retrieve**

Retrieves the bindings for the device.

**Clear IP Counter(s)**

Resets the IP Change Count to zero for the binding.

**Clear Binding(s)**

Removes the binding from the table.

---

**Related Information**

For information on related tasks:

- [How to Configure Anti-Spoofing](#)
- [Port Properties - Anti-Spoofing Tab](#)



## Arbiter Mode Tab (Transmit Queue Port Group)

---

The Arbiter Mode tab lets you configure the transmit queue arbiter mode for the selected transmit queue port group. A transmit queue port group may contain multiple port queue types (for example, 4-queue ports and 16-queue ports) depending on the type of devices on your network. Each port type requires separate arbiter mode configuration using the corresponding subtab. For example, the screenshot below shows an Arbiter Mode tab with the 4 Queue Ports subtab selected.

---

**NOTE:** The Arbiter Mode tab will display subtabs for all the port types supported by the devices on your network, regardless of whether the selected port group contains those port types or not.

---

The arbiter mode is the method used to determine the way that traffic in each queue is serviced. It is based on a percentage or weight (called a "slice") given to each queue.

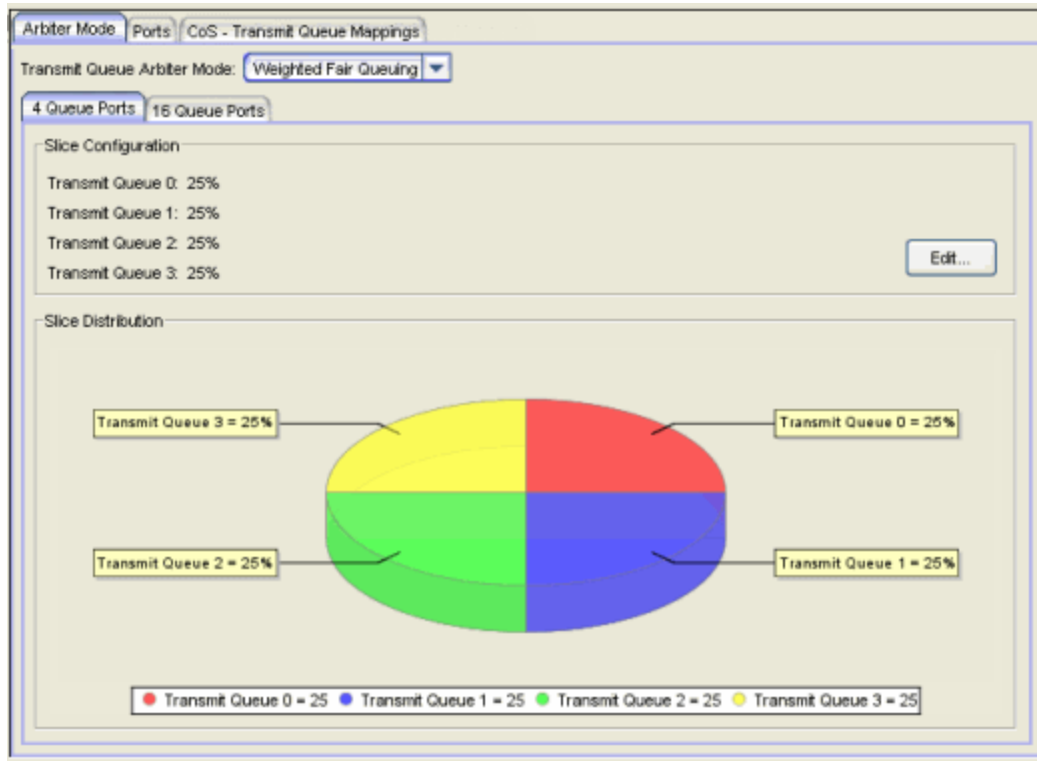
By default, ports are set to Strict mode, which means that the highest priority queue (the highest numbered queue) is set to 100%. In Strict mode, queues are serviced by numerical priority from the highest numbered queue to the lowest, and all frames in the highest priority queue will be transmitted before the frames in lower priority queues.

You can change the arbiter mode to Weighted Fair Queuing, which lets you adjust the slice percentage for each queue, and prevent a lower priority queue from being starved.

You can also select Enhanced Transmission Selection mode (ETS), which allows you to designate 2 or more traffic class queues as ETS queues. The scheduler will then service all non-ETS queues first using strict priority.

For more information on the arbiter mode, see [Transmit Queue Bandwidth Configuration](#).

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a transmit queue port group in the tree, and then select the Arbiter Mode tab in the right panel.



### Transmit Queue Arbiter Mode

The transmit queue arbiter mode determines the way that traffic in each queue is serviced. Use the drop-down list to select a mode:

- **Strict** - The highest priority queue (the highest numbered queue) is set to 100%. In strict mode, queues are serviced by numerical priority from the highest numbered queue to the lowest. Queues are serviced until empty or until a higher priority queue requires servicing. For example, for a 4-queue port in strict mode, all frames in Transmit Queue 3 will be transmitted before the frames in Transmit Queue 0.
- **Weighted Fair Queuing** - Queues are serviced according to the percentage or weight you assign to each queue. This prevents a lower priority queue from being starved. Percentages must add up to 100%. Configuring 100% for the highest priority queue sets the port to Strict mode.
- **Enhanced Transmission Selection (ETS)** - Allows you to designate 2 or more traffic class queues as ETS queues. The ETS queues are then assigned bandwidth allocation with the sum of the ETS queues bandwidth equaling 100%. The scheduler will then service all non-ETS queues first using strict priority. The remaining bandwidth is then distributed based on the allocation that was defined for each of the

ETS queues. The priorities within an ETS queue are serviced by strict priority.

- **Use Per-Port Type Arbiter Mode** - Allows you to specify an arbiter mode independently for each port type (for example, 11 Queue Ports or 16 Queue ports).

## Slice Configuration

Lists the slice percentages given to each queue on the port. Use the **Edit** button to open the [Edit Slice Percentages window](#) where you can configure the slice distribution for each queue.

### Edit Button

Opens the [Edit Slice Percentages window](#) where you can configure the slice distribution for each queue.

## Slice Distribution

Displays the distribution of slice percentages in a graphical format. Use the **Edit** button to change the configuration.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

For information on related windows:

- [Ports Tab \(Transmit Queue Port Group\)](#)
- [CoS - Transmit Queue Mappings Tab \(Transmit Queue Port Group\)](#)

## Authentication Tab (Device)

The device Authentication tab enables you to configure and change the [authentication](#) settings on the selected device. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect (see [How to Configure Ports](#)).

To access this tab, select a device on the left panel's Network Elements tab, then click the Authentication tab in the right panel.

The screenshot displays the 'Authentication' configuration page for a device. The interface is divided into several sections:

- General Settings:**
  - Authentication Type:** Radio buttons for 'None', 'Single User', and 'Multi-User'. 'Multi-User' is selected.
  - Single User:** A sub-section with checkboxes for 'RADIUS Authentication', '802.1X', 'MAC', '802.1X+MAC', 'Web-Based', and 'CEP'. 'Web-Based' is selected.
  - Multi-User:** A sub-section with checkboxes for 'Quarantine', '802.1X', 'Web-Based', 'MAC', 'CEP', and 'Auto Tracking'. 'Web-Based' and 'Auto Tracking' are selected.
- Authentication Status:** A dropdown menu set to 'Disabled'.
- Re-Auth Timeout Action:** A dropdown menu set to 'Terminate'.
- User Statistics:** A table showing user counts:

Maximum Number of Users:	2048
Current Number of Users: Total:	113
802.1X:	0
Web-Based:	0
MAC:	0
CEP:	0
Quarantine:	0
Auto Tracking:	113
- Multi-User Authentication Type Precedence:** A text field containing 'Quarantine / 802.1X / PWA / MAC / CEP / Auto Track' with a gear icon for editing.
- RFC3580 VLAN Authorization:** Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected.
- Global Authentication Settings:** A sub-section with tabs for 'General', 'Guest Networking', 'Web Login', and 'DNS'.
  - Guest Networking Status:** A dropdown menu set to 'RADIUS Auth'.
  - Guest Name:** A text field containing 'guest'.
  - Guest Password:** A text field containing '\*\*\*\*\*'.

'Apply' buttons are present at the bottom of the 'General Settings', 'RFC3580 VLAN Authorization', and 'Global Authentication Settings' sections.

## General Settings

### Authentication Type

Select the appropriate single user or multi-user authentication types, or None. Only options supported by the selected device will be available for selection. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User Authentication). Deselect all options to see what authentication types are supported by this device, or refer to the NetSight Firmware Support tables for information on the authentication types supported by each device type. When you choose an authentication type, the sections unrelated to that type of authentication are grayed out on this tab and on the [Port Properties Authentication Configuration tab](#) for the device's ports. If you choose None, authentication of all types is disabled on the device. For more information on the different types of authentication, see [Authentication Types](#).

---

**WARNING:** Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, will log off any currently authenticated users.

---

**NOTE: C2/B2 Devices.** Because C2/B2 devices let you enable all three authentication types at the device level, use the Multi-User section to configure authentication types even though the device only supports a single user (and an optional IP phone) per port. The order in which authentication types are enabled at the device level may affect authentication settings that are already configured on the port. Because of this, it is important to configure authentication types at the device level first, and then configure your port-level authentication settings second.

If you are configuring a single user and an IP phone, be sure to set the port-level "number of users allowed" setting to 2. You can do this via the Port Configuration Wizard or the [Port Properties Authentication Configuration tab, Authenticated User Counts subtab](#).

---

### Authentication Status

If you've selected an authentication type other than None, you can enable it here. The default is Disabled. Leaving Authentication Status disabled gives you the ability to configure and reconfigure authentication settings without affecting your network until authentication configuration is complete. If you have selected multiple authentication types, all of the authentication types selected will be enabled or disabled with this one setting.

**CAUTION:** Setting the authentication status to Enabled will affect communications through the front panel ports. Any front panel port being used for management should be set to inactive/default mode before setting authentication status to Enabled. If you select the Enabled button, an Authentication Status window appears, offering you choices for actions that will take effect on front panel ports when authentication status is enabled. These options are described in detail on the Authentication Status window. (If you choose the **Select Ports to set to Inactive/Default Role** option, the [Set Authentication Port Mode to Inactive/Default Role window](#) appears, where you can select the ports you wish to set to Inactive/Default Role.)

---

### Re-Auth Timeout Action

This setting defines the action for sessions that need to be re-authenticated if the RADIUS server re-authentication request times out. Select the **Terminate** option to terminate the session or the **None** option to allow the current session to continue without disruption.


### Maximum Number of Users

For devices with Multi-User as their configured authentication type. The maximum number of users that can be actively authenticated or have authentications in progress at one time on this device. You can specify the maximum number of users per port on the port's [Port Properties Authentication Configuration tab](#).

### Current Number of Users

For devices with Multi-User as their configured authentication type. The current number of users that are actively authenticated or have authentications in progress, or that the device is keeping authentication termination information for. Any unauthenticated traffic on the port is not included in this count.

### Multi-User Authentication Type Precedence

Displays the order in which the authentication types will be tried on the device, with the authentication type on the left having the highest precedence (it will be tried first). You can edit the precedence order by clicking the Edit button . In the Edit Precedence window, select the authentication type you want to position, and use the left or right arrow to arrange the types in the desired order of precedence. The order determined here is also reflected in the position of the options under [Authentication Type](#).

---

**WARNING:** Leaving the default precedence is recommended. In particular, changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type can cause problems.

---

**NOTE:** On E1 and E6/E7 devices, if both 802.1X and MAC authentication are enabled, it is possible for the device to receive a start or response 802.1X packet while a MAC authentication is in progress. If this happens, the device immediately terminates the MAC authentication, and the 802.1X authentication proceeds to completion. Regardless of the success of the 802.1X login attempt, no new MAC authentication logins may occur on the port until 1) the link is toggled; 2) the user executes an 802.1X logout; or 3) the 802.1X session is terminated administratively.

---

### Apply

Saves any change you made to the General settings.

## RFC3580 VLAN Authorization

RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. When RFC 3580 VLAN Authorization is enabled:

- devices that do **not** support policy, will tag packets with the VLAN ID.
- devices that do support policy and also support [Authentication-Based VLAN to Role Mapping](#), will classify packets according to the role that the VLAN ID maps to.

You can also enable and disable VLAN Authorization at the port level using the [Port Properties Authentication Configuration tab](#). If the device does not support RFC 3580, this section will be grayed out.

### VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected device.

### Apply

Saves any change you made to the VLAN Authorization setting.

## Global Authentication Settings Tab

This tab lets you set session timeout and session idle timeout values for each authentication type.

Session Timeout:		Session Idle Timeout:	
802.1X:	0 sec	802.1X:	300 sec
Web-Based:	0 sec	Web-Based:	300 sec
MAC:	0 sec	MAC:	300 sec
CEP:	0 sec	CEP:	300 sec
Quarantine:	0 sec	Quarantine:	300 sec
Auto Tracking:	0 sec	Auto Tracking:	300 sec

### Session Timeout

The maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied. This value may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send a session timeout value in its authentication response.

---

**NOTE:** Non-zero values are rounded to the nearest non-zero multiple of 10 by the device.

---

### Session Idle Timeout

The maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that no idle timeout will be applied. This value may be superseded by an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send an idle timeout value in its authentication response.

## Web Authentication Settings Tab

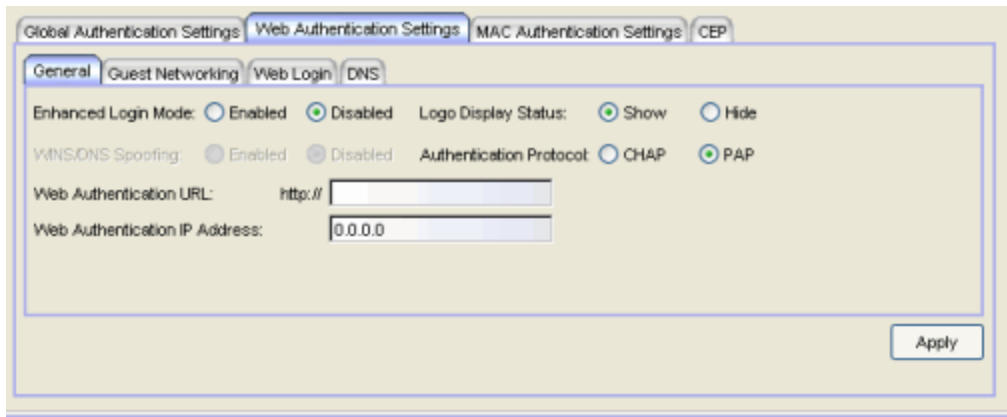
For users of web-based authentication, this tab lets you specify web authentication parameters using four sub-tabs: [General](#), [Guest Networking](#), [Web Login](#), and [DNS](#).

### *General Tab*

The General tab lets you specify the URL of the authentication web page and the IP address of the system where it resides. It also lets you enable certain web



authentication features such as Enhanced Login Mode, on devices that support those features.



### Enhanced Login Mode

Enabling the Enhanced Login Mode causes the authentication web page to be displayed regardless of whether the URL or IP address entered into the browser by the end user is the designated Web Authentication URL or IP address. This option is grayed out if the device does not support the mode.

### Logo Display Status

Specifies whether the Extreme Networks logo is displayed or hidden on the authentication web page window. This option is grayed out if not supported by the device.

### WINS/DNS Spoofing

Allows you to enable and disable WINS/DNS spoofing for the selected device. Spoofing allows the end user to resolve the Web Authentication URL name to the IP address using WINS/DNS. The default is Disabled. This option is grayed out if not supported by the device.

### Authentication Protocol

Authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to-Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

### Web Authentication URL

URL for your authentication web page. Users wishing to receive network services access the web page from a browser using this URL. The **http://** is

supplied. Alphabetical characters, numerical characters and dashes are allowed as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

### Web Authentication IP Address

IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the hosts file of each client.

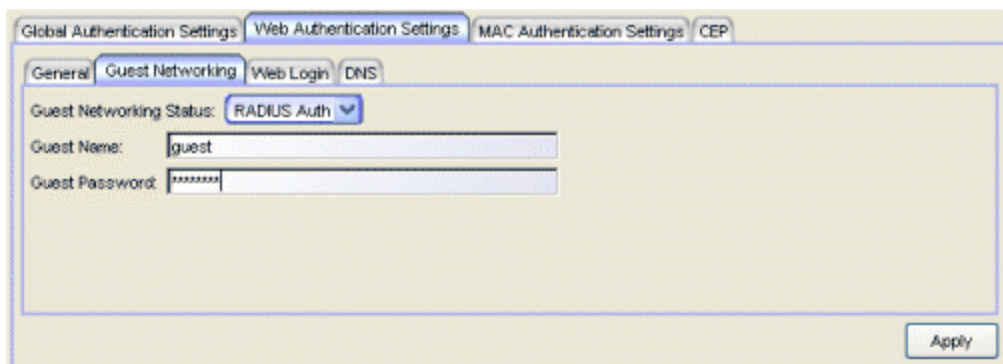
### *Guest Networking Tab*

The Guest Networking tab lets you configure guest networking, a feature that allows any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, allowing them to log in as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

---

**NOTE:** Guest networking is designed for networks using web-based authentication, with [port mode](#) set to Active/Discard.

---



### Guest Networking Status

Use the drop-down list to specify guest networking status:

- **Disable** -- Guest networking will be unavailable.
- **Local Auth** -- Guest Networking will be enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified [Guest Name](#). Once the user

submits the web page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.

- **RADIUS Auth** -- Guest Networking will be enabled. The user accesses the authentication web page, where the username field is automatically filled in with the specified [Guest Name](#), and the password field is masked out with asterisks. Once the user submits the web page using these credentials, the value of the [Guest Password](#) will be used for authentication. Following successful authentication from the RADIUS server, the port will apply the policy (role) returned from the RADIUS server. The port mode must be set to Active/Discard mode.

### Guest Name

The username that Guest Networking will use to authenticate users. The guest name is displayed automatically on the authentication web page. If the user does not want to log in as a guest, they can type in their valid username to override the guest username.

### Guest Password

The password that Guest Networking will use to authenticate users when [RADIUS Auth](#) is selected.

### Apply

Saves any change you made to the Guest Networking tab.

### Web Login Tab

The Web Login tab allows you to customize the banner end users see at the top of the authentication web page and set a Redirect Time, if applicable.

The screenshot shows the configuration page for the Web Login tab. At the top, there are tabs for 'Global Authentication Settings', 'Web Authentication Settings', 'MAC Authentication Settings', and 'CEP'. Under 'Web Authentication Settings', there are sub-tabs for 'General', 'Guest Networking', 'Web Login', and 'DNS'. The 'Web Login' sub-tab is active. The 'Web Page Banner' field contains the text: 'Enterasys Networks Incorporated', '9 Northeastern Boulevard', 'Salem, NH 03079', and '603 952-5000'. To the right of this field is a 'Default' button. Below the banner field is a 'Redirect Time (seconds):' field with the value '30'. At the bottom right of the configuration area is an 'Apply' button.

## Web Page Banner

Use this area to create a banner that end users will see at the top of the authentication web page. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it would not be appropriate to include "Welcome to [Your Company]" in the banner.

The **Default** button allows you to reset the banner to default text provided in a text file (pwa\_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa\_banner.txt file, located in the top level of the Policy Manager install directory. Then, when you click the Default button, the new text will be displayed in the Web Page Banner area.

## Redirect Time

For devices with [Enhanced Login Mode](#) enabled. Specifies the amount of time (in seconds) before the end user is redirected from the authentication web page to their requested URL.

An endstation using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. Redirect Time specifies the amount of time allowed for the end station to complete this process and begin using its official IP address. The default value of 30 seconds is adequate for most networks; however, some networks may require a longer or shorter time period. If the Redirect Time is not long enough, the browser times out while attempting to load the requested URL. In networks that only use static IP addresses, a Redirect Time of 5 to 10 seconds is usually sufficient; a value of less than 5 seconds is not recommended.

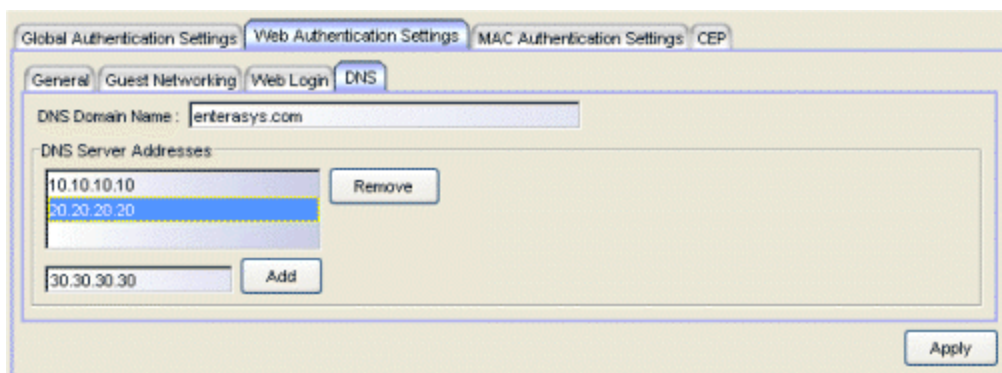
For example, if a user (in Enhanced Login Mode and a Redirect Time of 30 seconds) enters the URL of "http://ExtremeNetworks.com", they will be presented the authentication web page. When the user successfully authenticates into the network, they will see a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds".

## Default

Resets the authentication web page banner text to the default text provided in the text file, pwa\_banner.txt. The default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa\_banner.txt file, located in the top level of the Policy Manager install directory. Clicking Default also sets the Redirect Time field to the default value of 30 seconds.

## DNS Tab

The DNS tab lets you add your DNS domain name and server addresses to support the [Enhanced Login Mode](#) on Matrix E1 devices. Enhanced Login Mode must be enabled in order to use this tab. The DNS servers are used to resolve URLs to IP addresses.



### DNS Domain Name

Enter your local DNS Domain Name, for example, ExtremeNetworks.com.

### DNS Server Addresses

List your local DNS Server Addresses. Enter an IP address and click **Add** to add a server address. Select an address and click **Remove** to remove an address from the list. Addresses are used in the order they are listed.

## MAC Authentication Settings Tab

This tab enables you to set up the MAC password for [MAC authentication](#). In order for MAC authentication to work, you must also configure the RADIUS server with the MAC password as well as the MAC addresses which are allowed to authenticate.

The screenshot shows a configuration window with four tabs: 'Global Authentication Settings', 'Web Authentication Settings', 'MAC Authentication Settings', and 'CEP'. The 'MAC Authentication Settings' tab is active. It contains a checkbox labeled 'Set Password/Mask' which is unchecked. Below this, there are two input fields: 'MAC User Password' (empty) and 'MAC Mask' (containing 'FF:FF:FF:FF:FF:FF'). Below these fields is a dropdown menu for 'MAC Address Delimiter' set to 'Hyphen'. An 'Apply' button is located in the bottom right corner.

### MAC User Password

The password that is passed to the RADIUS server for MAC authentication (1-32 characters).

### MAC Mask

You can select a mask to provide a way to authenticate end stations based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturers ID portion of the MAC address. The MAC Mask is passed to the RADIUS server for authentication after the primary attempt to authenticate using the full MAC address fails.

### MAC Address Delimiter

The character used between octets in a MAC address:

- **None** — No delimiter is used in the MAC address (e.g. xxxxxxxxxxxx).
- **Hyphen** — A hyphen is used as a delimiter in the MAC address (e.g. xx-xx-xx-xx-xx-xx).

### Apply

Saves any change you made to the MAC Authentication Settings tab.

## CEP Tab

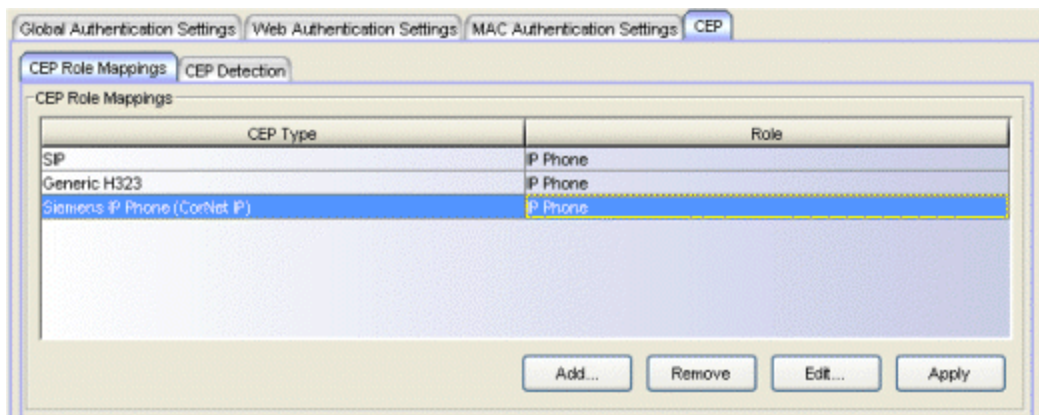
This tab provides a way to identify Convergence End Points (IP phones) that are connecting to the device, and apply a role to the endpoint based on the type of endpoint detected. The CEP Detection sub-tab lets you create detection rules for identifying the endpoints, and the CEP Role Mappings sub-tab lets you map a role to each CEP product type.

**TIP:** You can configure CEP for multiple devices using the [Device Configuration Wizard](#).

In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access sub-tab in the [Port Properties Authentication Configuration Tab](#) or the [Port Configuration Wizard](#). Once you have configured CEP on the device and each port, you can monitor CEP usage on the Port Usage Tab (Port) or Port Usage Tab (Device).

### *CEP Role Mappings Tab*

This tab lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence endpoint (such as an IP phone) connects to the network, the device identifies the type of endpoint (using CEP detection rules) and applies the assigned role.



### CEP Role Mappings

Lists the CEP types supported by the device and the role mapped to each type. Click **Add** to add a CEP type and role to the list.

### Add

Opens the Add CEP Mapping window where you can select a CEP product type supported on the device, and map a role for that type. Your selections will be added to the CEP Role Mappings list.

### Remove

To remove a CEP type in the CEP Role Mappings list, select the type and click **Remove**.

### Edit

To edit a CEP type in the CEP Role Mappings list, select the type and click **Edit**. The Edit CEP Mapping window opens where you can select a different CEP type and/or role.

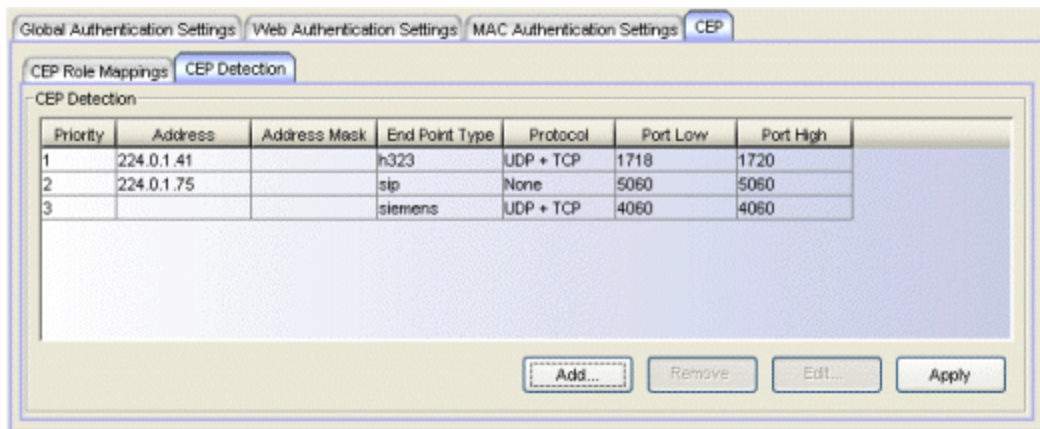
## CEP Detection Tab

Use this tab to create CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected.

**NOTE:** CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection - Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones will be detected on TCP/UDP port 4060.
- IP Address detection - H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules that will detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones will be detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones will be detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones will also be detected using only their respective multicast addresses without the TCP/UDP ports.



### Priority

The rule priority with one (1) being the highest priority. The rule with the highest priority will be used first, so it is recommended that the highest



priority be given to the predominate protocol in the network to provide for greater efficiency.

**Address**

If the rule is based on IP address detection, this field displays the IP address that incoming packets will be matched against. By default, H.323 will use 224.0.1.41 as its IP address, SIP will use 224.0.1.75 as its IP address, and Siemens will have no IP address configured.

**Address Mask**

If the rule is based on IP address detection, this field displays the IP address mask that incoming packets will be matched against.

**End Point Type**

Specifies the endpoint type that will be assigned (H.323, Siemens, or SIP) if incoming packets match this rule.

**Protocol**

If the rule is based on TCP/UDP port detection, this field displays the protocol type used for matching, using a port range defined with the Port Low and Port High values:

- UDP + TCP - Match the port number for both UDP and TCP frames.
- TCP - Match the port number only for TCP frames.
- UDP - Match the port number only for UDP frames.

**Port Low**

The low end of the port range defined for detection on UDP and/or TCP ports.

**Port High**

The high end of the port range defined for detection on UDP and/or TCP ports.

**Add**

Opens the [Add CEP Detection Rule window](#) where you can create CEP detection rules.

**Remove**

To remove a CEP detection rule, select the entry and click **Remove**.

**Edit**

To edit a CEP detection rule, select the rule and click **Edit**. The [Edit CEP Detection Rule window](#) opens where you edit the rule's parameters. You can also double-click an entry in the table to open the edit window.

## Related Information

For information on related tasks:

- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)

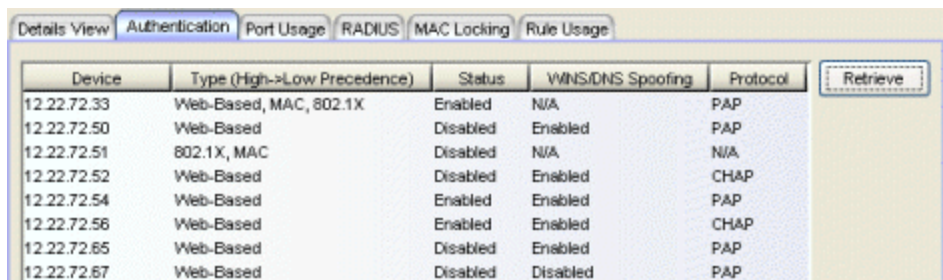
## Authentication Tab (Device Group/Island)

The Authentication tab displays the current [authentication](#) settings of the devices in the selected device group, Policy VLAN Island, or Network Resource Topology Island. To access this tab:

- select a device group in the left-panel Network Elements tab
- select a VLAN island in the left-panel of the Access Control Configuration window (available from the Policy Manager Edit menu)
- select a topology island in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu)

then click the Authentication tab in the right panel.

**TIP:** Use the [device Authentication tab](#) to configure authentication settings for an individual device.



Device	Type (High->Low Precedence)	Status	WINS/DNS Spoofing	Protocol	Retrieve
12.22.72.33	Web-Based, MAC, 802.1X	Enabled	N/A	PAP	
12.22.72.50	Web-Based	Disabled	Enabled	PAP	
12.22.72.51	802.1X, MAC	Disabled	N/A	N/A	
12.22.72.52	Web-Based	Disabled	Enabled	CHAP	
12.22.72.54	Web-Based	Enabled	Enabled	PAP	
12.22.72.56	Web-Based	Enabled	Enabled	CHAP	
12.22.72.65	Web-Based	Disabled	Enabled	PAP	
12.22.72.67	Web-Based	Disabled	Disabled	PAP	

### Device

Name or IP address of the device.

### Type

Authentication type(s) for the device (802.1x, MAC, or Web-Based), or None. If the value is None, authentication is disabled. For devices that support multiple authentication types, the authentication types are displayed in order of precedence, with the authentication type on the left having the highest precedence (it will be tried first). You can specify authentication type precedence on the device's [Authentication tab](#).

### Status

Indicates whether or not authentication is enabled on the device. If multiple authentication types are configured on the device, this status applies to all authentication types.

### **WINS/DNS Spoofing**

For web-based authentication, the WINS/DNS spoofing status of the device (Enabled or Disabled). Spoofing allows the end user to resolve the Web Authentication URL name to the IP address using WINS/DNS.

### **Protocol**

For web-based authentication, the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

### **Current Number of Users**

The current number of users that are actively authenticated or have authentications in progress, or that the device is keeping authentication termination information for.

### **Maximum Number of Users**

The maximum number of users that can be actively authenticated or have authentications in progress at one time. You can specify the maximum number of users per port on the [Port Properties Authentication Configuration tab](#).

### **Web Authentication URL**

For web-based authentication, the authentication login web page address.

### **Web Authentication IP**

For web-based authentication, the IP address of the system where the authentication login web page resides.

### **Web Authentication Logo Display**

For web-based authentication, indicates whether the Web Authentication Logo is displayed (show) or hidden (hide) on your Login Web Page Banner window. If the device does not support this option, the column will read N/A.

### **Enhanced Login Mode**

For web-based authentication, indicates whether Enhance Login Mode is enabled or disabled on the device. When Enhanced Login Mode is enabled, it causes the authentication web page to be displayed regardless of whether the URL entered into the browser by the end user is the Web Authentication URL or not.

### Retrieve Button

Retrieves the latest authentication information from the devices and displays it in the table.

---

### Related Information

For information on related concepts:

- [Authentication](#)

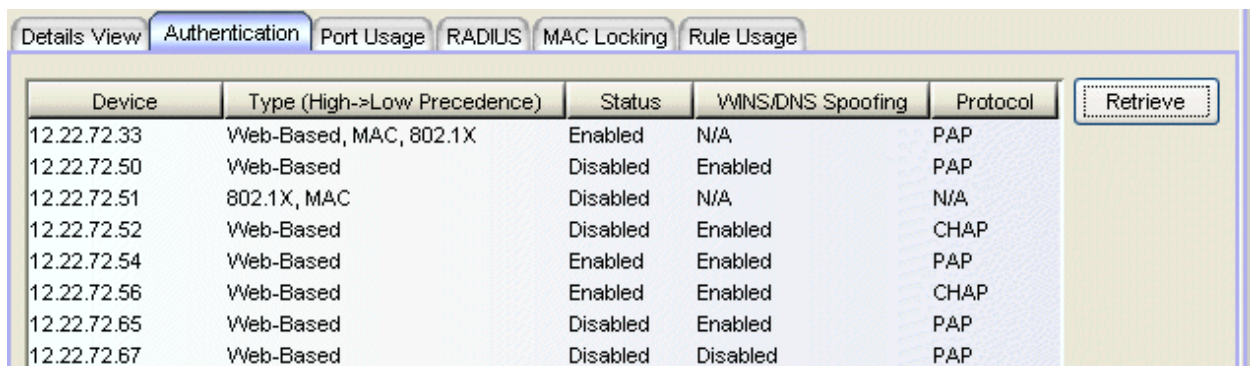
For information on related tasks:

- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)

## Authentication Tab (My Network/All Devices Folder)

The Authentication tab displays the current [authentication](#) settings of all the devices in the current domain. To access this tab, select either the My Network or the All Devices folder in the left-panel Network Elements tab, then click the Authentication tab in the right panel.

**TIP:** Use the [device Authentication tab](#) to configure authentication settings for an individual device.



Device	Type (High->Low Precedence)	Status	WINS/DNS Spoofing	Protocol	Retrieve
12.22.72.33	Web-Based, MAC, 802.1X	Enabled	N/A	PAP	
12.22.72.50	Web-Based	Disabled	Enabled	PAP	
12.22.72.51	802.1X, MAC	Disabled	N/A	N/A	
12.22.72.52	Web-Based	Disabled	Enabled	CHAP	
12.22.72.54	Web-Based	Enabled	Enabled	PAP	
12.22.72.56	Web-Based	Enabled	Enabled	CHAP	
12.22.72.65	Web-Based	Disabled	Enabled	PAP	
12.22.72.67	Web-Based	Disabled	Disabled	PAP	

### Device

Name or IP address of the device.

### Type

Authentication type(s) for the device (802.1X, MAC, or Web-Based), or None. If the value is None, authentication is disabled. For devices that support multiple authentication types (such as the N-Series), the authentication types are displayed in order of precedence, with the authentication type on the left having the highest precedence (it will be tried first). You can specify authentication type precedence on the device's [Authentication tab](#).

### Status

Indicates whether or not authentication is enabled on the device. If multiple authentication types are configured on the device, this status applies to all authentication types.

### **WINS/DNS Spoofing**

For web-based authentication, the WINS/DNS spoofing status of the device (Enabled or Disabled). Spoofing allows the end user to resolve the Web Authentication URL name to the IP address using WINS/DNS.

### **Protocol**

For web-based authentication, the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

### **Current Number of Users**

For N-Series devices. The current number of users that are actively authenticated or have authentications in progress, or that the device is keeping authentication termination information for.

### **Maximum Number of Users**

For N-Series devices. The maximum number of users that can be actively authenticated or have authentications in progress at one time. You can specify the maximum number of users per port on the [Port Properties Authentication Configuration tab](#).

### **Web Authentication URL**

For web-based authentication, the authentication login web page address.

### **Web Authentication IP**

For web-based authentication, the IP address of the system where the authentication login web page resides.

### **Web Authentication Logo Display**

For web-based authentication, indicates whether the Web Authentication Logo is displayed (show) or hidden (hide) on your Login Web Page Banner window. If the device does not support this option, the column will read N/A.

### **Enhanced Login Mode**

For web-based authentication, indicates whether Enhance Login Mode is enabled or disabled on the device. When Enhanced Login Mode is enabled, it causes the authentication web page to be displayed regardless of whether the URL entered into the browser by the end user is the Web Authentication URL or not.

### Retrieve Button

Retrieves the latest authentication information from the devices and displays it in the table.

---

### Related Information

For information on related concepts:

- [Authentication](#)

For information on related tasks:

- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)



## CoS - Rate Limit Mappings Tab (Rate Limit)

This tab lists all the rate limit port groups using the selected rate limit, along with their rate limit mapping information. Rate limit mappings map a logical rate limit index (IRL/ORL Index) to an actual physical rate limit. You can configure a port group's mappings on the port group [Mappings tab](#).

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a rate limit in the tree, and the CoS - Rate Limit Mappings tab will be displayed in the right panel.

Direction	Port Group	IRL/ORL Index	Rate Limit	
Inbound	Default	3	5 Mb/s [Prec: 2]	[8 Rate Limit Ports, 32 F...

### Direction

Specifies whether the rate limit is for inbound or outbound traffic. Inbound rate limiting takes place after a frame has been classified into one of the eight priorities. Outbound rate limiting takes place just before a frame is queued for transmission.

### Port Group

The name of the port group using this rate limit.

### IRL/ORL Index

The logical rate limit index number.

### Rate Limit

The actual rate limit that the IRL/ORL index is mapped to. In this case, it will be the rate limit selected in the left-panel tab.

### Port Type

The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).

### Rate Used By CoS

The class of service using this rate limit.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [Creating Class of Service Port Groups](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)
- [CoS - Rate Limit Mappings Tab \(Rate Limit Port Group\)](#)

## CoS - Rate Limit Mappings Tab (Rate Limit Port Group)

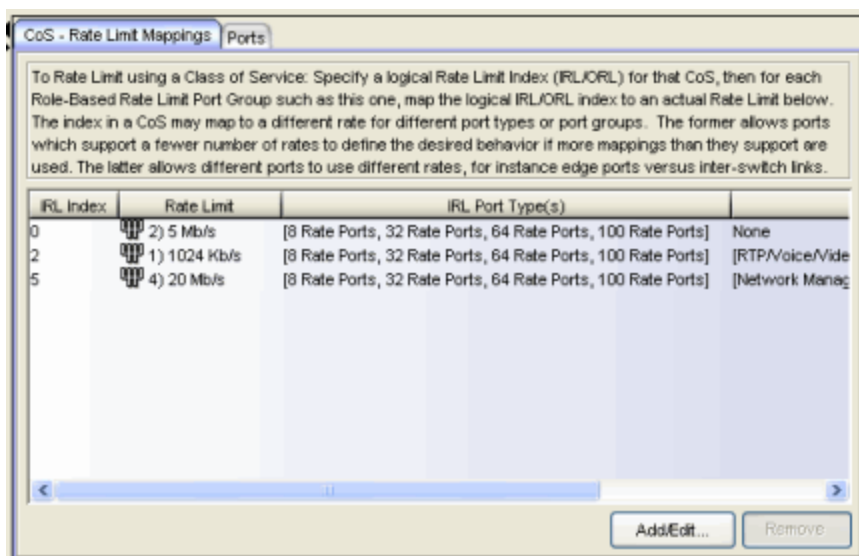
This tab lets you view and configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index used by classes of service to an actual physical rate limit you have created in Policy Manager.

Each port group has its own set of index mappings. Policy Manager automatically assigns these index numbers when you configure a class of services's rate limits and transmit queue shapers.

The rate limit mappings tab allows you to do two things:

- Map the index to a different rate for different port groups (edge ports versus inter-switch links). See [Creating Class of Service Port Groups](#)
- Map the index to a different rate limit for each port type (8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit) in a port group. See [Advanced Rate Limiting by Port Type](#).

To access this tab, select a rate limit port group in the left-panel of the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a rate limit port group in the tree and then select the CoS - Rate Limit Mappings tab in the right panel.



### IRL/ORL Index

The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming packets. For each rate limit port group, use this tab to map the index number to an actual rate limit.

### Rate Limit

The actual rate limit that the IRL/ORL index is mapped to.

### IRL/ORL Port Type(s)

The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).

### IRL/ORL Index Used By CoS

The classes of service using this IRL/ORL index.

### Add/Edit Button

Opens the [Add/Edit CoS to Rate Limit Mappings window](#) where you can add or edit rate limit mappings for the rate limit port group

### Remove Button

Removes the mapping(s) selected in the table.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Define Rate Limits](#)
- [Advanced Rate Limiting by Port Type](#)

For information on related windows:

- [Ports Tab \(Rate Limit Port Group\)](#)

## CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group)

---

This tab lets you view and configure the transmit queue mappings for a transmit queue port group. Transmit queue mappings map a logical transmit queue index used by classes of service to an actual physical transmit queue you have configured in Policy Manager.

Some devices can have ports that support different numbers of transmit queues (for example, 4 transmit queue ports and 16 transmit queue ports). The mappings for each port type is configured here in this tab. For 4-, 8-, and 11-transmit queue ports, the number of indexes (0-15) is greater than the actual number of transmit queues the ports support. For example, in the graphic below you can see the default mappings for the 4-queue ports: 16 transmit queue indexes (0-15) are mapped to four physical queues (0-3).

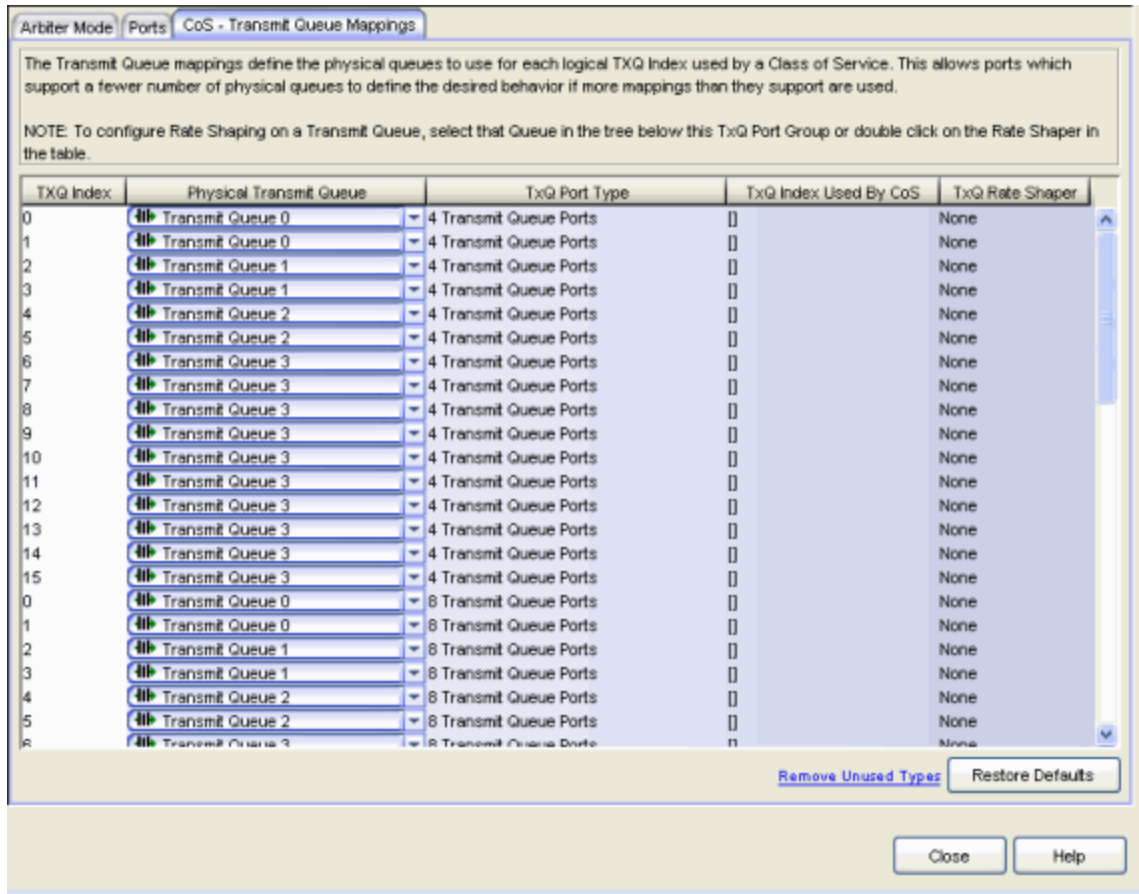
When you first open the tab you will see the default mapping for the port group's transmit queues. Changing this mapping allows you to fine tune the transmit queue configuration according to the needs of the selected transmit queue port group, and utilize any [rate shaping values](#) you may have assigned to the transmit queues.

---

**TIP:** Double-click on an entry in the table to open the transmit queue's General tab where you can configure rate shaping for the transmit queue.

---

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a transmit queue port group in the tree, and then select the CoS - Transmit Queue Mappings tab in the right panel.



**TXQ Index**

The logical transmit queue index. This index number is specified in a class of service and dictates the queue and shaping behavior for incoming packets. For each transmit queue port group, use this tab to map the index number to an actual physical transmit queue.

**Transmit Queue Index Mapping**

Use the drop-down lists to select the physical transmit queue you would like to map to each transmit queue index.

**TXQ Port Type**

Port type is based on the number of transmit queues the port supports: 4 transmit queues or 16 transmit queues.

**TXQ Index Used By CoS**

The Class of Service using this TXQ index.

**TXQ Rate Shaper**

The transmit queue's associated rate shaper as configured in the transmit queue's General tab.

### Restore Defaults

Click this button to restore the default transmit queue mappings for the port group.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

For information on related windows:

- [Arbiter Mode Tab \(Transmit Queue Port Group\)](#)
- [Ports Tab \(Transmit Queue Port Group\)](#)

## Flood Control Rate Limits Tab (Flood Control Port Groups)

---

This tab allows you to set individual flood control rates for each traffic type (Unicast, Multicast, and Broadcast). You can also create a new rate limit or edit an existing rate.

Choices include:

- None
- [Create Rate Limit/Shaper](#)
- [Edit Rate Limit/Shaper\(s\)](#)

As flood control is enabled/disabled for a Class of Service, when enabled, each column will either display a rate limit, or "None", if no rate has been defined for that portion of flood control.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Expand Flood Control Groups, and select a flood control port group in the tree. The Flood Control Rate Limits tab will be displayed in the right panel.



Flood Control Rate Limits Ports

To use Flood Control for a Class of Service, enable Flood Control for that CoS. All CoS with Flood Control enabled will use the same FC configuration defined in each Flood Control Port Group.

Flood Control Rates

Unicast Unknown: 1) 1024 Kb/s

Multicast: 2) 5 Mb/s

Broadcast: 3) 10 Mb/s

Close Help

### Unicast Unknown

Select a rate, create a new rate, or edit an existing flood control rate limit for Unicast traffic.

### Multicast

Select a rate, create a new rate, or edit an existing flood control rate limit for Multicast traffic.

### Broadcast

Select a rate, create a new rate, or edit an existing flood control rate limit for Broadcast traffic.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Configure Flood Control](#)

- [How to Create a Rate Limit](#)
- [How to Edit a Rate Limit](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)

## Details View Tabs

---

Some Details View tabs display a simple list of items for the current selection in the left panel. However, other Details View tabs present more complex tables of information. To access Help topics on those tabs, expand the Details View Tabs folder in the Policy Manager Help Table of Contents. The Help topics are named to reflect the item selected in the left-panel tree. For example, the Help topic for the Details View tab with a device selected in the left panel is named Details View Tab (Device).

Most Details View tabs provide the following features:

- *Right-click menus:* Right-click an item for a menu of options.
- *Drag and drop:* Populate services and service groups in the left panel by dragging and dropping multiple selections from the right-panel Details View lists. For example, in the right panel Details View for a service, you can select a rule and drag it into another service in the left panel.
- *Sorting, filtering and finding:* Clicking on column headings sorts the column. Right-clicking on column headings opens a menu enabling you to perform [sort](#), [filter](#), and [find](#) operations.
- *Double-click opening:* Double-clicking an item opens a tab containing more information about the item, often the Details View tab detailing the components of the item, or the General tab for the item.

---

### Related Information

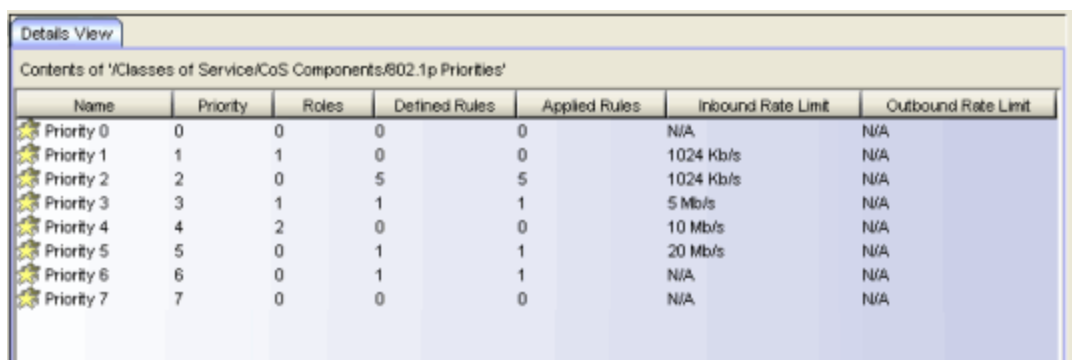
For information on related tasks:

- [How to Filter, Find, and Sort](#)

## Details View Tab (802.1p Priorities Folder)

This tab displays a table of information about the eight priorities defined in the 802.1p specifications, and how they are being used in Policy Manager. It appears when you select the 802.1p Priorities folder in the left panel of the Class of Service Configuration window (available from the Policy Manager Edit menu).

The listed priorities have values of 0-7 (with 7 being the highest priority), and are used to determine the order in which network traffic will be transmitted.



The screenshot shows a window titled 'Details View' with a subtitle 'Contents of \'Classes of Service/CoS Components/802.1p Priorities\''.

Name	Priority	Roles	Defined Rules	Applied Rules	Inbound Rate Limit	Outbound Rate Limit
Priority 0	0	0	0	0	N/A	N/A
Priority 1	1	1	0	0	1024 Kb/s	N/A
Priority 2	2	0	5	5	1024 Kb/s	N/A
Priority 3	3	1	1	1	5 Mb/s	N/A
Priority 4	4	2	0	0	10 Mb/s	N/A
Priority 5	5	0	1	1	20 Mb/s	N/A
Priority 6	6	0	1	1	N/A	N/A
Priority 7	7	0	0	0	N/A	N/A

### Name

Name of the 802.1p priority.

### Priority

Priority ranking of the 802.1p priority (0-7, with 7 being the highest priority).

### Roles

Number of roles associated with the 802.1p priority.

### Defined Rules

Total number of rules utilizing this 802.1p priority. This includes rules that are enabled and are part of at least one role (applied rules), as well as rules not yet assigned to any roles.

### Applied Rules

Number of rules utilizing this 802.1p priority that are enabled and are part of at least one role.

### Inbound Rate Limit

The priority-based inbound rate limit associated with the priority, if any. Otherwise, N/A. The rate limit sets the highest rate of speed at which traffic can enter a port before packets will be dropped.

### Outbound Rate Limit

The priority-based outbound rate limit associated with the priority, if any. Otherwise, N/A. The rate limit sets the highest rate of speed at which traffic can exit a port before packets will be dropped.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)

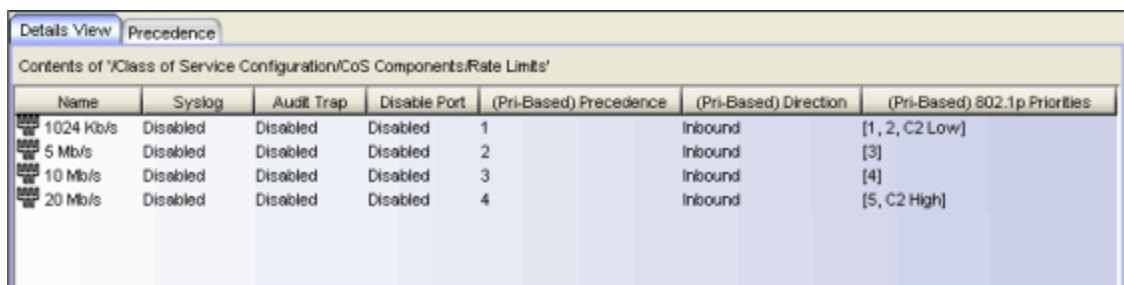
For information on related windows:

- [General Tab \(802.1p Priority\)](#)

## Details View Tab (Rate Limits Folder)

This tab lists information on any rate limits that have been defined in Policy Manager. Double-click on a rate limit in the list to open the rate limit's General tab.

To access this tab, select the Rate Limits folder in the left panel of the Class of Service Configuration window (available from the Policy Manager Edit menu), then select the Details View tab in the right panel. See [How to Define Rate Limits](#) for more information.



The screenshot shows a window titled 'Details View' with a sub-tab 'Precedence'. The main content area is titled 'Contents of "/>

### Name

Name of the rate limit.

### Syslog

Specifies whether a syslog message will be generated when the rate limit is first exceeded.

### Audit Trap

Specifies whether an audit trap will be generated when the rate limit is first exceeded.

### Disable Port

Specifies whether the port will be disabled when the rate limit is first exceeded.

### (Pri-Based) Precedence

The order in which priority-based rate limits will be written to devices that support them. Policy Manager allows you to define as many priority-based rate limits as you wish; however, the number written to a device is restricted by the number of rate limits supported by the device. See [Precedence Tab \(Rate Limits Folder\)](#) for more information.

---

**NOTE:** Although all rate limits have a precedence and show up in this list, only rate limits that include a priority-based configuration will actually be written to a device.

---

#### (Pri-Based) Direction

Indicates whether the priority-based rate limit is for inbound or outbound traffic.

#### (Pri-Based) 802.1p Priorities

Rate limits with a priority-based rate limit configuration will display the 802.1p priorities (0-7, with 7 being the highest priority) associated with the rate limit. Rate limits with only a role-based rate limit configuration will display "None."

---

### Related Information

For information on related windows:

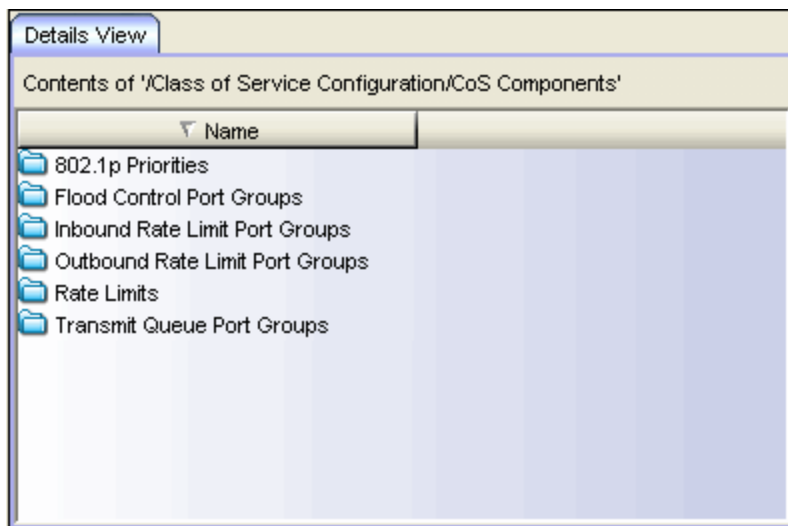
- [General Tab \(Rate Limit\)](#)

## Details View Tab (CoS Components Folder)

---

This tab lists the elements that can comprise a class of service. It appears when you select the CoS Components folder in the left panel tree of the Class of Service Configuration window (available from the Policy Manager Edit menu).

See [Getting Started with Class of Service](#) for more information about these components.



---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

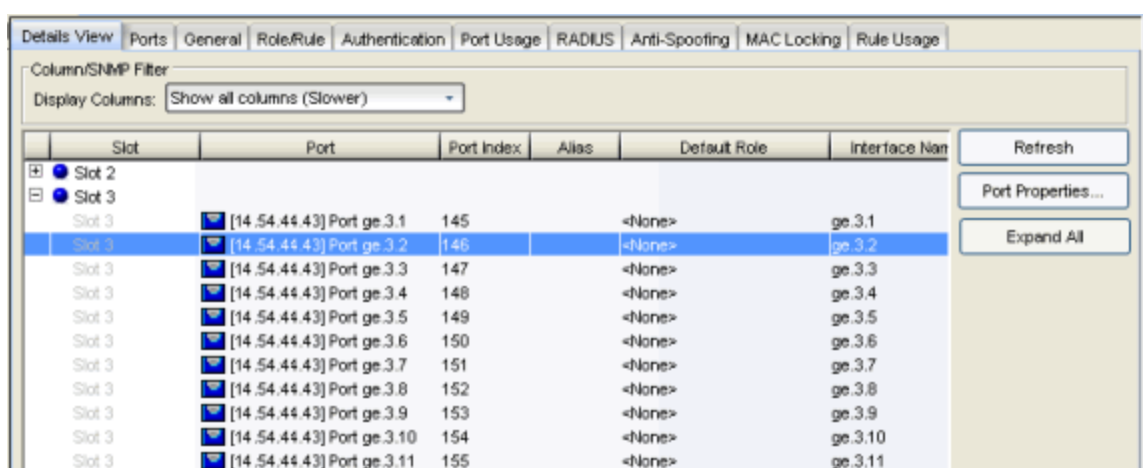
- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)
- [How to Configure Flood Control](#)



## Details View Tab (Device)

This tab appears when you select a device in the left-panel Network Elements tab. Multi-module devices will display slot numbers according to which slots have modules in them, and a Logical Ports grouping (if you have the Hide Logical Ports feature deselected in the Options view.) Stand-alone devices and single-module devices will simply display a Ports grouping.

Expand a slot or ports grouping to display a table of information about the ports on the device. To see a menu of options available for a port, right-click the port.



### Column/SNMP Filter

Port data retrieval requires many SNMP queries and can cause significant wait times to fill in the requested port details view. High network latency environments are most impacted by the delay. Use this menu to hide unnecessary columns to improve performance by reducing SNMP overhead.

- **Show all columns (Slower)** - Lets you view all port details.
- **Show only basic columns (Fastest)** - Hides some columns of information to lower SNMP overhead and allow faster retrieval times of port data.
- **Show optional columns (Faster)** - Display one or more of the hidden columns by selecting an optional column checkbox.

### Slot

Multi-module devices display slot numbers according to which slots have modules in them, and a Logical Ports grouping (if you have the Hide Logical Ports feature deselected in the Options view.) Stand-alone devices and single-module devices will simply display a Ports grouping.

**Port**

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

**Port Index**

The index value assigned to the port interface.

**Alias**

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

**Default Role**

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

**Interface Name**

A description of the port.

**Egress Policy**

Displays whether [egress policy](#) is enabled, disabled, or not supported (N/A) for the port.

**Port Type**

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

**Port Speed**

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

**Port Mode**

[Port mode](#) as set in the port's [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

**Device Auth Mode**

Authentication type(s) configured on the device ([Quarantine](#), [802.1X](#), [Web-Based](#), [MAC](#), [CEP](#), [Auto Tracking](#), or None). Some devices support multiple authentication types and multiple users (Multi-User authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User authentication). If the value is None, all types of authentication are disabled at the device level, and port authentication settings cannot be configured and will not take effect.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

### TCI Overwrite

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

### MAC Locking

Indicates whether or not [MAC locking](#) is enabled on the port.

### Refresh Button

Updates the contents of the table.

### Port Properties Button

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

### Expand All Button

Expands all slot or port groups.

---

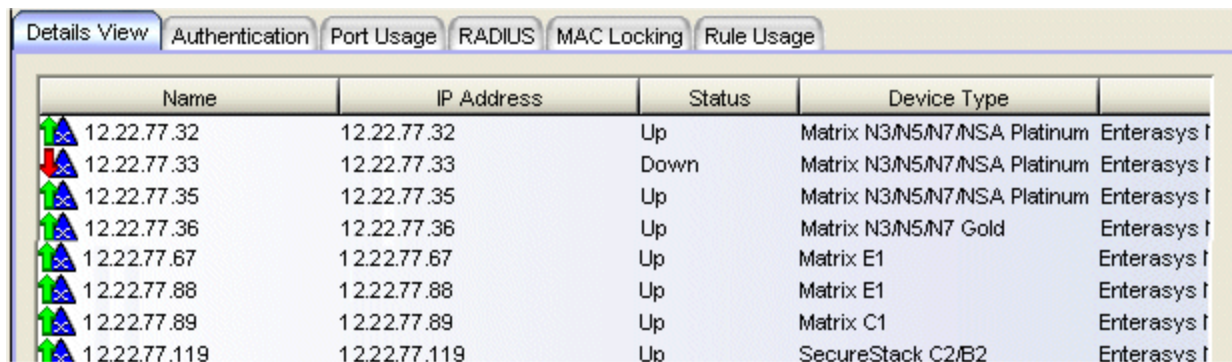
## Related Information

For information on related windows:

- [Ports Tab \(Device\)](#)

## Details View Tab (Device Group)

This tab is displayed when you select a device group from the left-panel Network Elements tab. It displays a table of information about the devices in the device group. If you right-click a device in the table, a menu of available options appears.



The screenshot shows a software interface with a tabbed menu at the top containing 'Details View', 'Authentication', 'Port Usage', 'RADIUS', 'MAC Locking', and 'Rule Usage'. The 'Details View' tab is active, displaying a table with the following columns: Name, IP Address, Status, and Device Type. The table contains eight rows of data, each with a small icon to the left of the Name column. The icons are green with a blue triangle pointing up (indicating 'Up') or red with a blue triangle pointing down (indicating 'Down').

Name	IP Address	Status	Device Type
12.22.77.32	12.22.77.32	Up	Matrix N3/N5/N7/NSA Platinum
12.22.77.33	12.22.77.33	Down	Matrix N3/N5/N7/NSA Platinum
12.22.77.35	12.22.77.35	Up	Matrix N3/N5/N7/NSA Platinum
12.22.77.36	12.22.77.36	Up	Matrix N3/N5/N7 Gold
12.22.77.67	12.22.77.67	Up	Matrix E1
12.22.77.88	12.22.77.88	Up	Matrix E1
12.22.77.89	12.22.77.89	Up	Matrix C1
12.22.77.119	12.22.77.119	Up	SecureStack C2/B2

### Name

Name of the device, or its IP address if it does not have a name.

### IP Address

The device's IP address.

### Status

The device's current operational status.

### Device Type

Indicates the type of device. Certain devices may be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

### Firmware Version

Shows the current firmware revision for this device.

### Class of Service Mode

Shows the current class of service mode setting for this device:

- Rate Limits Disabled - Rate limiting is disabled on this device. This means that any priority-based rate limits will not be written to the device on enforce, and any role-based rate limits will not be included in roles written to devices on enforce.

- Role-Based Rate Limits/Transmit Queue Configuration - This setting means that you are able to configure role-based rate limits and transmit queues on this device. See [Defining Role-Based Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.
- Priority-Based Rate Limits - This setting means that you are able to configure priority-based rate limits on this device. See [Defining Priority-Based Rate Limits](#) for more information.

When a device is set to configure a subset of the domain level's CoS managed components (using the Device Managed CoS Components field on the device General tab), a message is added to this column, for example, "(Ignore CoS components: IRL/ORL)".

---

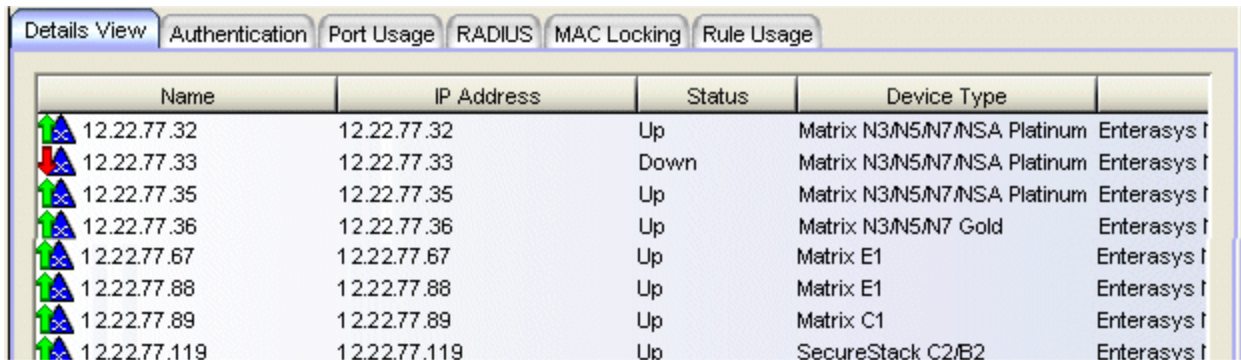
### **Related Information**

For information on related windows:

- [Details View Tabs](#)

## Details View Tab (My Network/All Devices Folder)

This Details View tab displays a table of information about all the devices in the current domain. To access this tab, select either the My Network or the All Devices folder in the left-panel Network Elements tab. The Details View is displayed in the right panel. To see a menu of options available for a device, right-click the device.



The screenshot shows a software interface with a tabbed menu at the top containing 'Details View', 'Authentication', 'Port Usage', 'RADIUS', 'MAC Locking', and 'Rule Usage'. The 'Details View' tab is active, displaying a table with the following columns: Name, IP Address, Status, and Device Type. Each row represents a device with its corresponding IP address, status, and device type.

Name	IP Address	Status	Device Type
12.22.77.32	12.22.77.32	Up	Matrix N3/N5/N7/NSA Platinum
12.22.77.33	12.22.77.33	Down	Matrix N3/N5/N7/NSA Platinum
12.22.77.35	12.22.77.35	Up	Matrix N3/N5/N7/NSA Platinum
12.22.77.36	12.22.77.36	Up	Matrix N3/N5/N7 Gold
12.22.77.67	12.22.77.67	Up	Matrix E1
12.22.77.88	12.22.77.88	Up	Matrix E1
12.22.77.89	12.22.77.89	Up	Matrix C1
12.22.77.119	12.22.77.119	Up	SecureStack C2/B2

### Name

Name of the device, or its IP address if it does not have a display name.

### IP Address

The device's IP address.

### Status

The device's current operational status.

### Device Type

Indicates the type of device. Certain devices may be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

### Firmware Version

Shows the current firmware revision for this device.

### Class of Service Mode

Shows the current class of service mode setting for this device:

- Rate Limits Disabled - Rate limiting is disabled on this device. This means that any priority-based rate limits will not be written to the device on enforce, and any role-based rate limits will not be included in roles written to devices on enforce.

- Role-Based Rate Limits/Transmit Queue Configuration - This setting means that you are able to configure role-based rate limits and transmit queues on this device. See [Defining Role-Based Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.
  - Priority-Based Rate Limits - This setting means that you are able to configure priority-based rate limits on this device. See [Defining Priority-Based Rate Limits](#) for more information.
- 

## Related Information

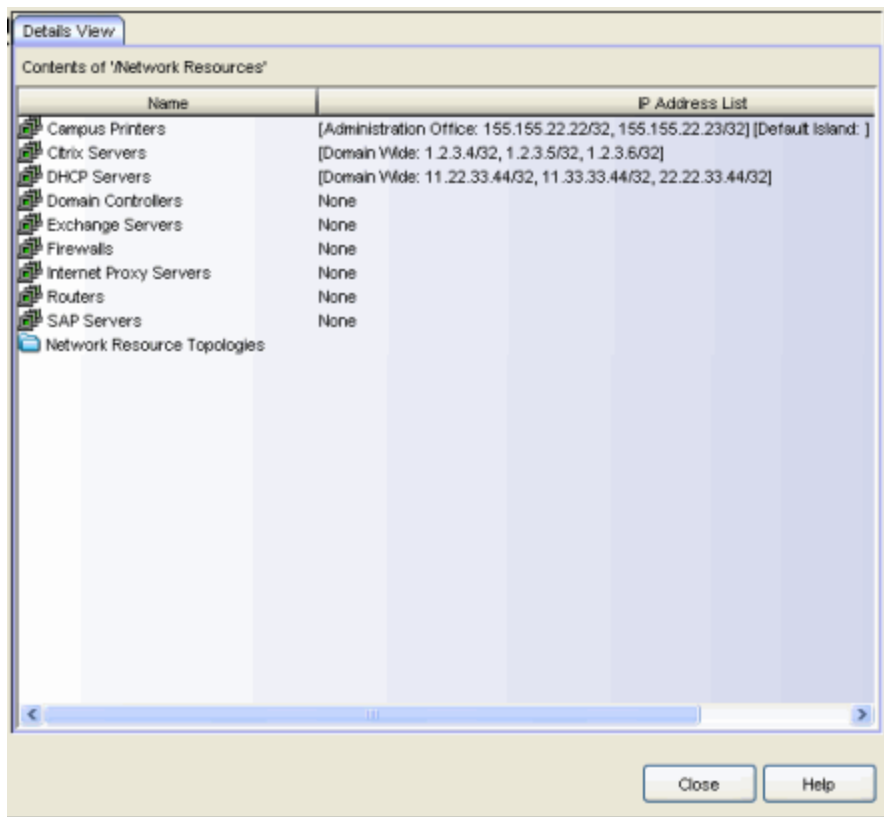
For information on related windows:

- [Details View Tabs](#)

## Details View Tab (Network Resources Folder)

This tab appears when you select the Network Resource folder in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu). It displays a table of information about the network resource groups in the current domain.

Network resource groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. Once a network resource group has been defined, you can associate it with an [Automated service](#) (see [How to Create a Service](#) for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each device in the network resource group.



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of "/>

### Name

Name of the network resource group.



### Resource Address List

This column lists the [network resource topology](#) islands associated with the network resource group, followed by a list of the resources assigned to each island.

---

### Related Information

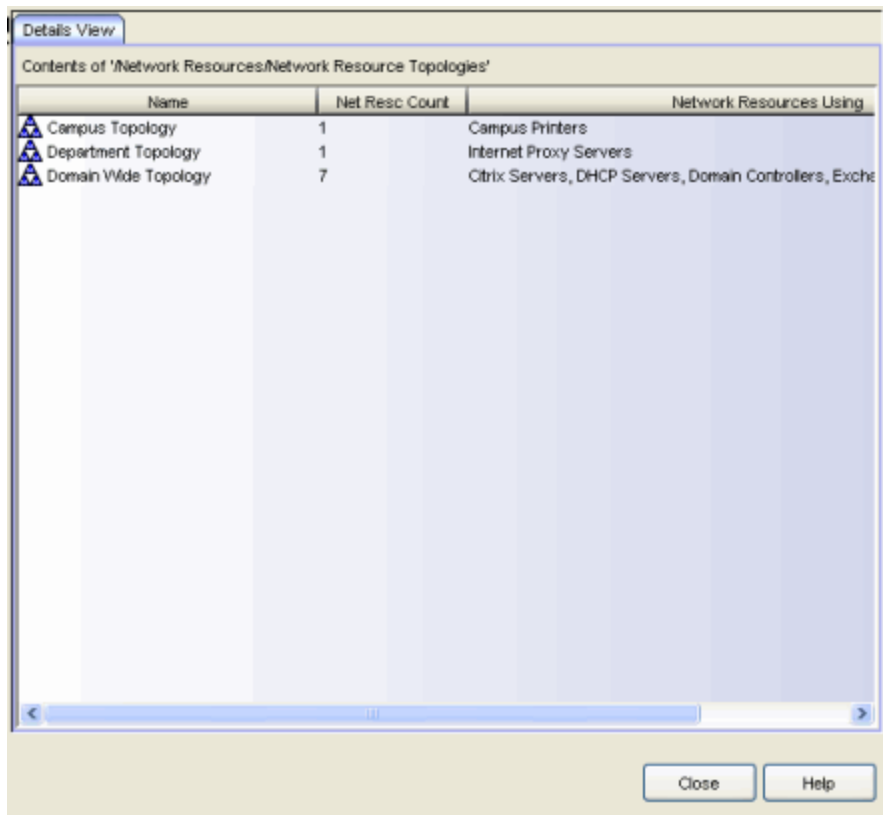
For information on related windows:

- [General Tab \(Network Resource Group\)](#)

## Details View Tab (Network Resource Topologies Folder)

---

This tab appears when you select the Network Resource Topologies folder in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu). It displays a table of information about the [network resource topologies](#) configured in the current domain. See [How to Create a Network Resource](#) for more information on topologies.



The screenshot shows a window titled 'Details View' with a subtitle 'Contents of "/>

### Name

Name of the network resource topology.

### Net Resc Count

The number of network resource groups using this topology.

### Network Resources Using

The names of the network resource groups using this topology.

---

## Related Information

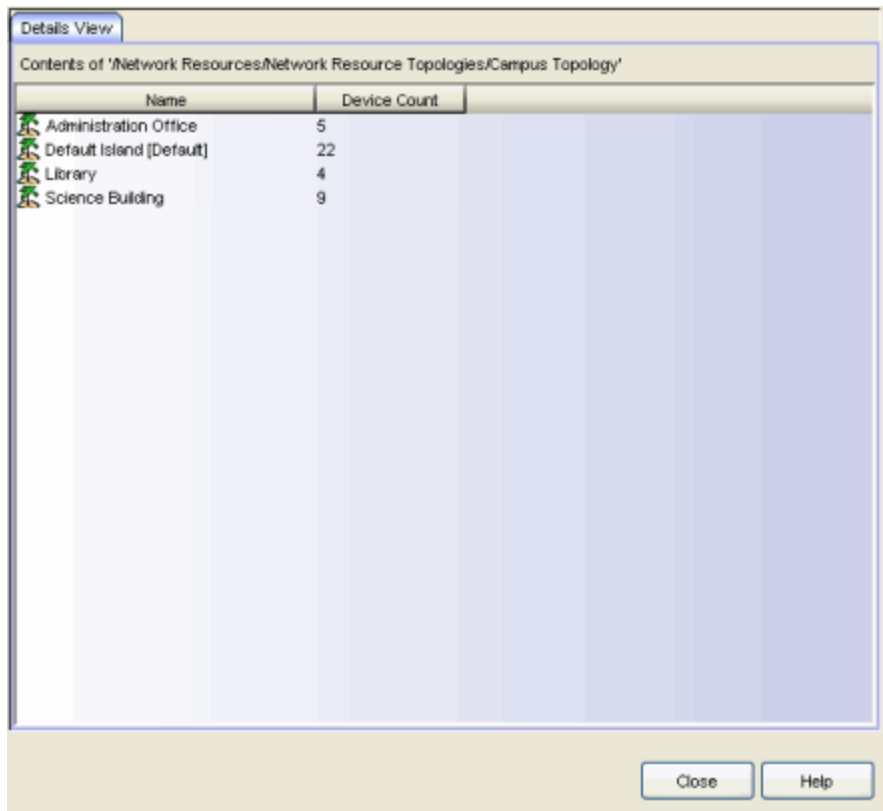
For information on related windows:

- [General Tab \(Network Resource Group\)](#)
- [How to Create a Network Resource](#)

## Details View Tab (Network Resource Topology)

---

This tab appears when you select a [Network Resource Topology](#) in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu). It displays a list of the islands defined for the topology and the number of devices assigned to each island. See [How to Create a Network Resource](#) for more information on topologies and islands.



The screenshot shows a window titled 'Details View' with a subtitle 'Contents of "/>

### Name

Name of the topology island.

### Device Count

The number of devices included in that island.

---

## Related Information

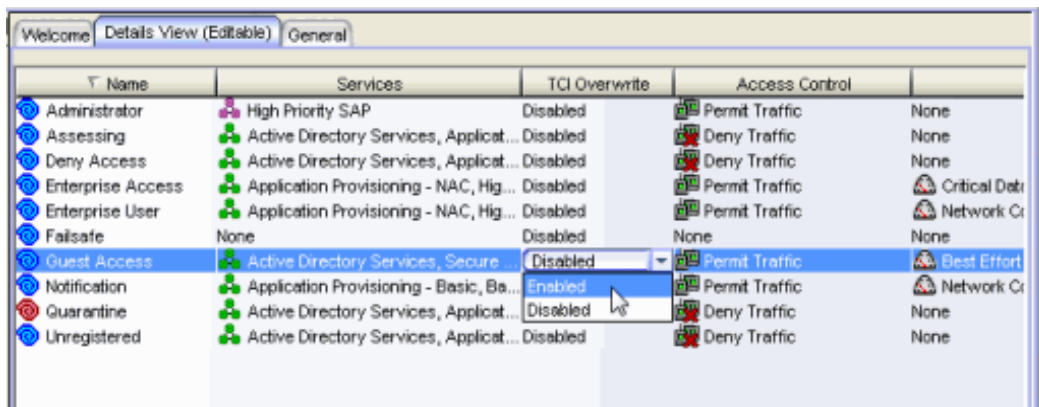
For information on related windows:

- [General Tab \(Network Resource Group\)](#)
- [How to Create a Network Resource](#)

## Details View Tab (Roles Folder)

This tab displays information about all the existing roles in the current domain. To see a menu of options available for a role, right-click the role. To access this tab, select the Roles folder in the left panel's Roles tab and click the Details View tab in the right panel.

The information in this Details View is editable. You can double-click on any of the table columns to edit a role's values using a combo box of available choices (as shown in the image below). Double-clicking on the Name column selects the role in the tree and opens the role's [General tab](#).



### Name

The name of the role.

### Services

The names of the services and service groups (local and global) associated with the selected role.

### TCI Overwrite

Whether TCI Overwrite is enabled or disabled for the role. Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this role or any of its rules to overwrite the VLAN or class of service (CoS) tag in a received packet if that packet has already been tagged with VLAN or CoS information. If TCI Overwrite is not enabled, tagged packets will egress using the TCI data they already contain.

### Access Control

The default access control associated with the role. Possible values are Permit Traffic, Deny Traffic, Contain to VLAN, or None.

**CoS**

The default class of service associated with the role. Possible values are the name of a class of service or None.

**System Log**

Whether the System Log default action is enabled or disabled. When enabled, a syslog message is generated as long as no matching rules specify that sending a syslog message is prohibited (that is, the rule's system log action is set to "Prohibited" on the [Rule General tab](#)). When disabled, the system log setting is ignored.

**Audit Trap**

Whether the Audit Trap default action is enabled or disabled. When enabled, an audit trap is generated as long no matching rules specify that sending an audit trap is prohibited (that is, the rule's audit trap action is set to "Prohibited" on the [Rule General tab](#)). When disabled, the audit trap setting is ignored.

**Disable Port**

Whether the Disable Port default action is enabled or disabled. When enabled, the port is disabled as long no matching rules specify that disabling the port is prohibited (that is, the rule's disable port action is set to "Prohibited" on the [Rule General tab](#)). Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#). When disabled, the disable port setting is ignored.

**Traffic Mirror**

Whether the Traffic Mirror default action is enabled or disabled. For more information, see [traffic mirroring](#).

**Number of Rules**

The number of traffic classification rules the role includes.

---

**Related Information**

For information on related windows:

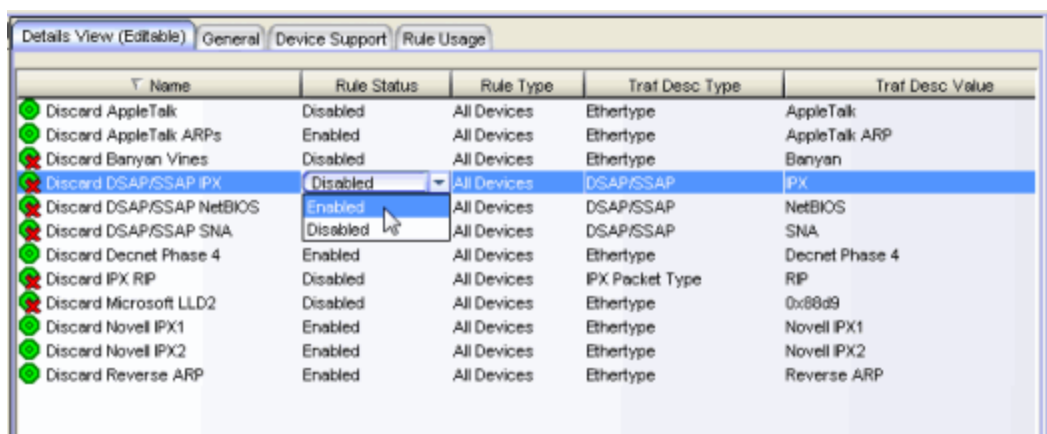
- [General Tab \(Role\)](#)

## Details View Tab (Service)

This tab displays information about the rules contained in a [Manual service](#) or an [Automated service](#). To display this tab, select a service in the left-panel's Services tab and select the Details View tab in the right panel. Right-click a rule in the table to see a menu of available options.

For Manual services, you can double-click on any of the table columns to edit a rule's values (as shown in the image below). Double-clicking on the Traf Desc Value column lets you open the [Edit Rule window](#) where you can change the traffic description associated with the rule. Double-clicking the other columns displays a combo box of available choices. Double-clicking on the Name column selects the rule in the tree and opens the rule's [General tab](#).

**TIP:** You can easily add a rule to a service by dragging and dropping a rule from this Details View tab to a service in the left-panel tree.




Name	Rule Status	Rule Type	Traf Desc Type	Traf Desc Value
Discard AppleTalk	Disabled	All Devices	Ethertype	AppleTalk
Discard AppleTalk ARPs	Enabled	All Devices	Ethertype	AppleTalk ARP
Discard Banyan Vines	Disabled	All Devices	Ethertype	Banyan
Discard DSAP/SSAP IPX	Disabled	All Devices	DSAP/SSAP	IPX
Discard DSAP/SSAP NetBIOS	Enabled	All Devices	DSAP/SSAP	NetBIOS
Discard DSAP/SSAP SNA	Disabled	All Devices	DSAP/SSAP	SNA
Discard Decnet Phase 4	Enabled	All Devices	Ethertype	Decnet Phase 4
Discard IPX RIP	Disabled	All Devices	IPX Packet Type	RIP
Discard Microsoft LLD2	Disabled	All Devices	Ethertype	0x88a9
Discard Novell IPX1	Enabled	All Devices	Ethertype	Novell IPX1
Discard Novell IPX2	Enabled	All Devices	Ethertype	Novell IPX2
Discard Reverse ARP	Enabled	All Devices	Ethertype	Reverse ARP

### Name

Name of the rule. For rules contained in an Automated service, this column gives detailed information about the rule including the associated Network Resource (NR), if multiple resource groups are specified.

### Rule Status

Indicates whether the rule is currently available for use by this service (Enabled), or not (Disabled), as set in the [General tab](#) for the rule, or in the Rule Status window of the [Service Wizard](#) or [Classification Rule Wizard](#). If the rule is disabled, the rule icon displays a red X .



**Rule Type**

Indicates the device types to which the rule applies. (See [Create Classification Rule Window](#) for more information.)

**Traf Desc Type**

Traffic classification type for the rule. (See [Classification Types and their Parameters](#) for more information.)

**Traf Desc Value**

Values associated with the traffic classification type for the rule. (See [Classification Types and their Parameters](#) for more information.) Double-clicking on this column opens the [Edit Rule window](#), where you can edit the parameters or values for the rule's classification type.

**Access Control**

VLAN action associated with the rule. Double-clicking on this column allows you change the setting. You can permit traffic to be forwarded, deny traffic altogether, or select a VLAN to contain traffic. Select **None** to disable access control for this rule.

**CoS**

Class of service action associated with the rule. Double-clicking on this column allows you change the setting.

**Sys Log on Rule Hit**

Displays whether the syslog functionality (a syslog message is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

**Trap on Rule Hit**

Displays whether the audit trap functionality (an audit trap is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

### Disable Port on Rule Hit

Displays whether the disable port functionality (ports reported as using this rule will be disabled) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
- **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

### Traffic Mirror

Displays whether the [traffic mirror](#) functionality is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Select port group(s)** - Use the drop-down list to specify the port groups where mirrored traffic will be sent for monitoring and analysis.
- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

### TCI Overwrite

Displays whether TCI Overwrite is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

### Quarantine Role

Displays whether a [Quarantine role](#) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Select Role** - Use the drop-down list to select the role that you want to assign as a Quarantine role.
  - **Disabled** - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.
- 

### Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related windows:

- [General Tab \(Rule\)](#)
- [Rule Usage Tab \(Rule\)](#)

## Details View Tab (Services Folder)

---

This tab lists the Automated and Manual services you have created in Policy Manager. To display the tab, expand the Local Services or Global Services folders in the left-panel Services tab, and select the Services folder. To see a menu of options available for a service, right-click the service.

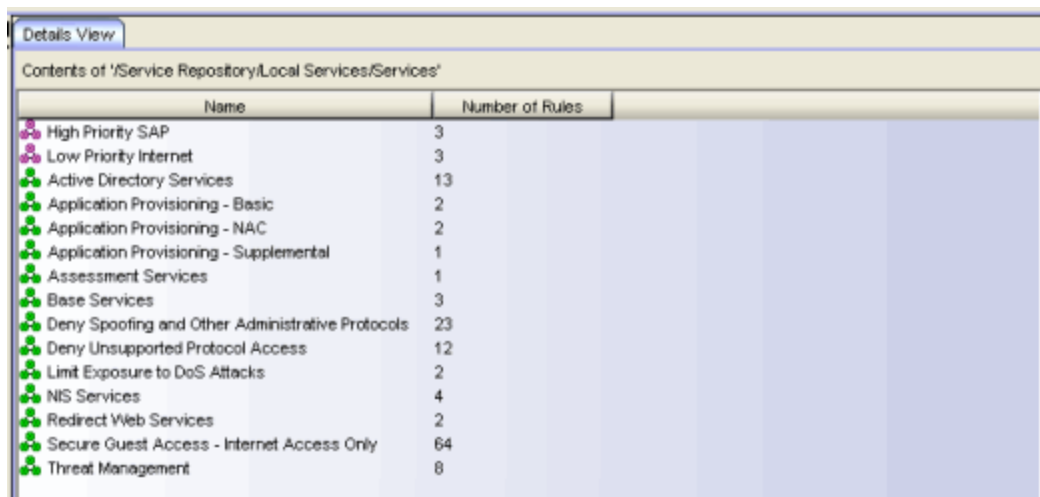
For information on the differences between automated or manual services, and local or global services, see the Policy Manager Concepts Help topic's section on [Services](#).

---

**TIPS:** - **Add service to service group.** You can easily add a service to a service group by dragging and dropping a service from this Details View tab to a service group in the left-panel tree.

- **Add service to role.** You can add one or more services to a role by right-clicking a service and selecting Add to Role(s) from the menu. This opens the Add to Role window where you can select the roles to which you want to add the services.

---



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of "/>

### Name

Name of the service.

### Number of Rules

Number of rules associated with the service.

---

## Related Information

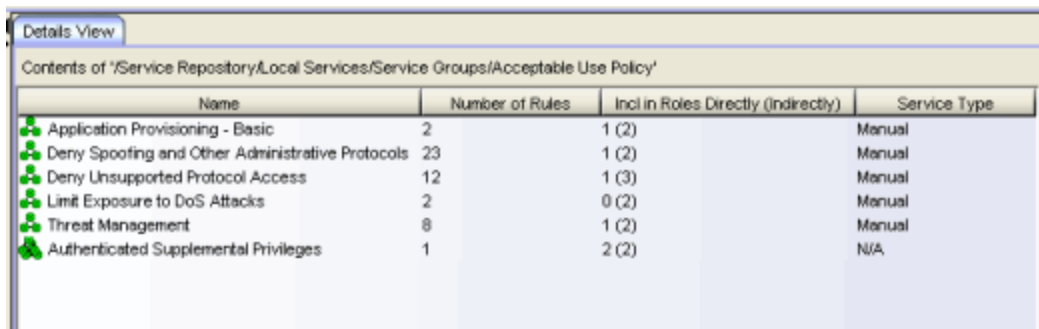
For information on related tasks:

- [How to Create a Service](#)

## Details View Tab (Service Group)

This tab lists information about the services or service groups contained in a Local or Global service group. To display this tab, select a service group in the left-panel Services tab.

**TIP:** Use drag and drop to quickly copy a service or service group from this Details View tab to another service group in the left-panel tree.



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of "/>

### Name

The name of the service or service group.

### Number of Rules

The number of rules included in the service or service group.

### Incl in Roles Directly (Indirectly)

The number of roles where the service or service group exists directly in the role's Services list (as viewed on the role's [General tab](#)). If a service group also exists indirectly in other roles as part of another service group, that number of roles is displayed in parenthesis. In the example above, the service group called "Authenticated Supplemental Privileges" displays "1 (1)" in this column, showing that it is associated directly with one role (exists in that role's services list) and is also part of a service group associated with one other role.

### Service Type

Indicates whether the service is [Manual](#) or [Automated](#). For service groups, this column will display N/A.

### Network Resources

If the service is [Automated](#), the network resource group(s) to which it applies. Otherwise, N/A (Not Applicable).

**VLAN**

If the service is [Automated](#), the name of the VLAN with which the service is associated, if applicable. Otherwise, N/A (Not Applicable).

**Class of Service**

If the service is [Automated](#), the name of the class of service with which the service is associated, if applicable. Otherwise, N/A (Not Applicable).

**Parent Service Group(s)**

Displays all the "parent" service groups to which the service or service group belongs. This gives you an idea of the service group hierarchy without having to expand the left-panel tree.

---

**Related Information**

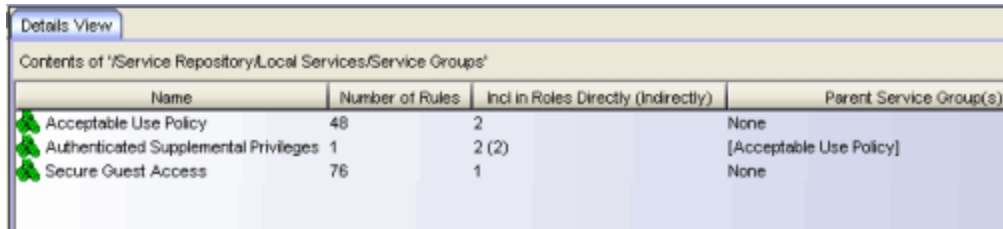
For information on related tasks:

- [How to Create a Service](#)

## Details View Tab (Service Groups Folder)

---

This tab appears when you select the Service Groups folder on the left panel's Services tab. It displays a table of information about the existing service groups. To see a menu of options available for a service group, right-click the service group.



The screenshot shows a window titled 'Details View' with a subtitle 'Contents of "/>

### Name

The name of the service group.

### Number of Rules

The number of rules included in the service group.

### Incl in Roles Directly (Indirectly)

The number of roles where the service group exists directly in the role's Services list (as viewed on the role's [General tab](#)). If the service group also exists indirectly in other roles as part of another service group, that number of roles is displayed in parenthesis. In the example above, the service group called "Authenticated Supplemental Privileges" displays "2 (2)" in this column, showing that it is associated directly with two roles (exists in that role's services list) and is also part of a service group associated with two other roles.

### Parent Service Group(s)

If the service group is part of another service group, this column displays that "parent" service group. In the example above, the service group called "Authenticated Supplemental Privileges" is part of the Acceptable Use Policy service group.

---

## Related Information

For information on related tabs:

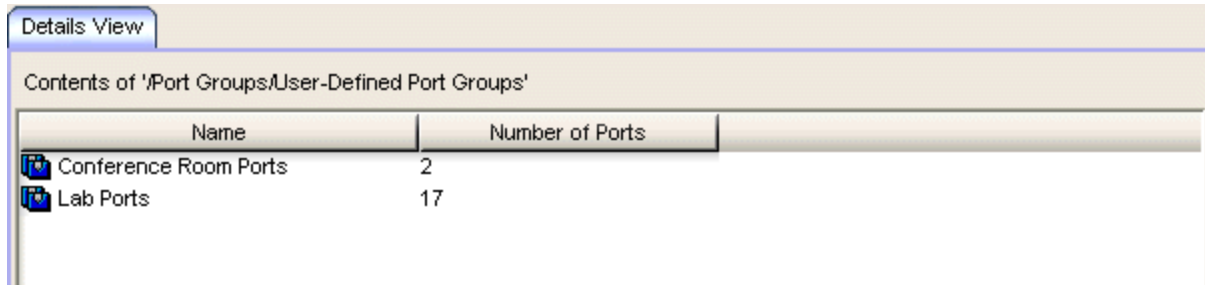
- [Role General Tab](#)



## Details View Tab (User-Defined Port Groups Folder)

---

This tab appears when you select the User-Defined Port Groups folder on the left-panel Port Groups tab. It displays a table of information about the existing port groups. To see a menu of options available for a port group, right-click the port group.



The screenshot shows a window titled 'Details View' with a subtitle 'Contents of '/Port Groups/User-Defined Port Groups''. Below the subtitle is a table with two columns: 'Name' and 'Number of Ports'. The table contains two rows of data: 'Conference Room Ports' with 2 ports and 'Lab Ports' with 17 ports.

Name	Number of Ports
Conference Room Ports	2
Lab Ports	17

### Name

Name of the port group.

### Number of Ports

Number of ports in the user-defined port group.

---

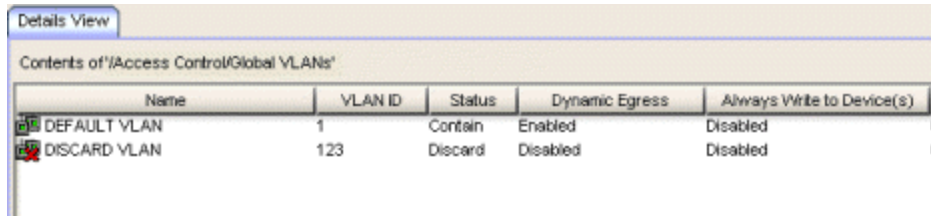
## Related Information

For information on related windows:

- [Details View Tabs](#)

## Details View Tab (VLANs Folder)

This tab appears when you select the Global or Island VLANs folder in the left panel of the Access Control Configuration window (available from the Policy Manager Edit menu). It displays a table of information about the existing VLANs. If you right-click an item in the table, a menu of available options appears.



The screenshot shows a window titled 'Details View' with a sub-header 'Contents of "/>


### Name

Name of the VLAN.

### VLAN ID

Unique number assigned to the VLAN, also called VID (for VLAN ID). For [Global VLANs](#), this ID was either assigned by an administrator or assigned automatically by the system when the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN). [Island VLANs](#) are conceptual and do not have actual VIDs (see [Policy VLAN Islands](#) for more information).

### Status

Indicates whether this VLAN is being used to deny traffic (Discard), or contain traffic (Contain). The icon for a Discard VLAN displays a red X .

### Dynamic Egress

Indicates whether the Dynamic Egress feature is on (Enabled) or off (Disabled) for the VLAN. The default is Enabled; therefore, this column will display Enabled unless a user has turned it off for a particular VLAN.

### Always Write to Device(s)

If enabled, the VLAN will be written to the device whether or not it is being used in a rule or role.

### Roles

Total number of roles associated with the VLAN.

### Defined Rules

Total number of rules associated with the VLAN, including [Applied Rules](#), as well as those not yet assigned to any roles.

### Applied Rules

Number of rules associated with this VLAN that are enabled and are part of at least one role.

---

### Related Information

For information on related windows:

- [Details View Tabs](#)

## Device Support Tab (Role)


Use the role Device Support tab to view the classification rule information that would be written to your device(s), should you decide to [enforce](#) the selected role. The information is displayed according to device type, and is particularly useful if you have devices that only support certain aspects of policy management.

To access this tab, select a role in the left panel Roles tab, then select the Device Support tab in the right panel.

The screenshot displays the 'Device Support' tab in a network management interface. The interface is divided into several sections:

- General Tab:** Includes 'General', 'VLAN Egress', 'Mappings', 'Ports', 'Device Support', and 'Rule Usage'.
- Devices:** A list of devices with their support status:
  - C2/B2/D2 - Rule(s) Not Fully Supported
  - C3/B3/G3 - Rule(s) Not Fully Supported
  - I-Series I3 - Rule(s) Not Fully Supported
  - Matrix C1 - Rule(s) Not Fully Supported
  - Matrix E1 - Supported
  - Matrix E5 - Rule(s) Not Fully Supported
  - Matrix E6/E7 - Supported
  - Matrix N3/N5/N7/NSA Platinum - Supported
  - Matrix N3/N5/N7 Gold - Rule(s) Not Fully Supported (highlighted with a yellow warning icon)
  - 10.20.10.20 (IP address)
  - Matrix X - Rule(s) Not Fully Supported
  - RoomAbout AP4000 - Rule(s) Not Fully Supported
- Classification Rules:** Divided into 'Excluded' and 'Included' sections.
  - Excluded:** A table with columns 'Name' and 'Traf Desc Typ'. It lists several 'Deny Spoofing and Other Administrative Pr...' rules with red 'X' icons, and two 'Deny Unsupported Protocol Access' rules with green checkmark icons.
  - Included:** A table with columns 'Name', 'Precedence', 'Traf Desc Type', and 'Traf Desc Value'. It lists several 'Deny Spoofing and Other Administrative Pr...' rules with green checkmark icons, and several 'Threat Management : Discard TCP Src' rules with green checkmark icons.
- Unmatched Frames:** A section at the bottom showing 'CoS: Priority 3' and 'Access Control: Permit Traffic'.

## Devices Area

This section displays folders for different device types. Expand the folders to see your network devices and device groups organized according to device type. If the domain does not include any devices of a specific device type, that device type folder is displayed in gray. For those device types that are included in the domain, the device type folders are displayed in black when the rule(s) are fully supported, and red when they are not fully supported. In addition, the  icon alerts you that there are certain rules that will not be written to this device type if you enforce, that you might want to investigate.

Select a specific device type to display the classification rules that will and/or will not be written to those devices when you [enforce](#) the selected role.

## Classification Rules Area

Based on the device type selected, this section displays the classifications rules that will be included or excluded when you enforce the selected role.

---

**TIP:** Double-clicking a rule in this table opens the rule's General tab, where you can easily edit a rule's parameters. This is particularly useful for editing unsupported rules.

---

### Excluded

Lists any unsupported classification rules. These rules will not be included when you enforce the selected role.

**NOTE:** Disabled rules  are always listed as Excluded.

---

### Included

Lists any supported classification rules. These rules will be included when you enforce the selected role.

**NOTE:** On S-Series and N-Series Platinum devices, range classification rules are achieved through applying subnet masks to values. As such, in order to achieve a user-specified range, the device may need multiple rules with subnets applied to encompass that range. So, although the user created only one rule with a range, this list may show multiple instances of that rule with the name of the rule followed by the portion of the over-all range it applies to.

---

---

## Excluded Table/Included Table

---

**TIP:** Double-clicking a rule in this table opens the rule's General tab, where you can easily edit a rule's parameters. This is particularly useful for editing unsupported rules.

---

### Name

The name of the service the rule belongs to, followed by the name of the rule.

### Precedence

The rule's precedence, with 1 being the highest precedence and 15 being the lowest. Rule precedence is based on classification type. When a role has multiple classification rules assigned to a port, rule precedence must be determined. For more information on precedence, see [Classification Rules Precedence](#). This column is only displayed in the Included table.

### Traffic Description Type

Displays the rule's classification type. See [Classification Types and their Parameters](#) for information.

### Traffic Description Value

Displays the values/parameters selected for the rule's classification type. See [Classification Types and their Parameters](#) for parameter information.

### Mask

The mask for the classification type, if applicable.

### Access Control

The access control (VLAN membership) action specified for the rule.

### CoS

The class of service (CoS) action specified for the rule.

### Precedence Help Button

Opens a Help topic on [Classification Rules Precedence](#).

## Unmatched Frames

This section displays the role's default Class of Service (CoS) and Access Control that will be applied to traffic received on the device that does not match any of the classification rules. These default actions can be viewed and edited in the role's [General tab](#).

## Related Information

For information on related concepts:

- [Enforcing](#)

For information on related windows:

- [Enforce Preview Window](#)

## Device Support Tab (Rule)

---

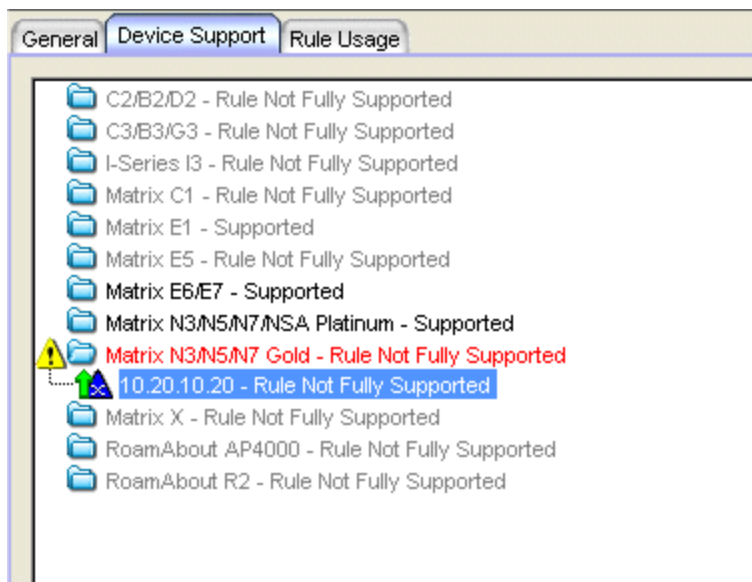
Use the rule Device Support tab to see whether or not the selected rule would be written to a device if you were to [enforce](#) a role with which the rule is associated. The information is displayed according to device type. If the domain does not include any devices of a specific device type, that device type folder is displayed in gray. For those device types that are included in the domain, the device type folders are displayed in black when the rule is supported, and red when it is not supported. This tab is particularly useful if you have devices that only support certain aspects of policy management.

To access this tab, select a rule in the left-panel Services tab, then select the right-panel Device Support tab.

---

**NOTE:** For Layer 2 MAC Address, Layer 3, and Layer 4 rules, a Matrix E1 device will be listed as supported if the rule's Access Control is set to Permit Traffic or Deny Traffic, but if the Access Control is set to Contain to VLAN, then the Matrix E1 will be listed as not supported.

---



### Related Information

For information on related concepts:



- [Enforcing](#)

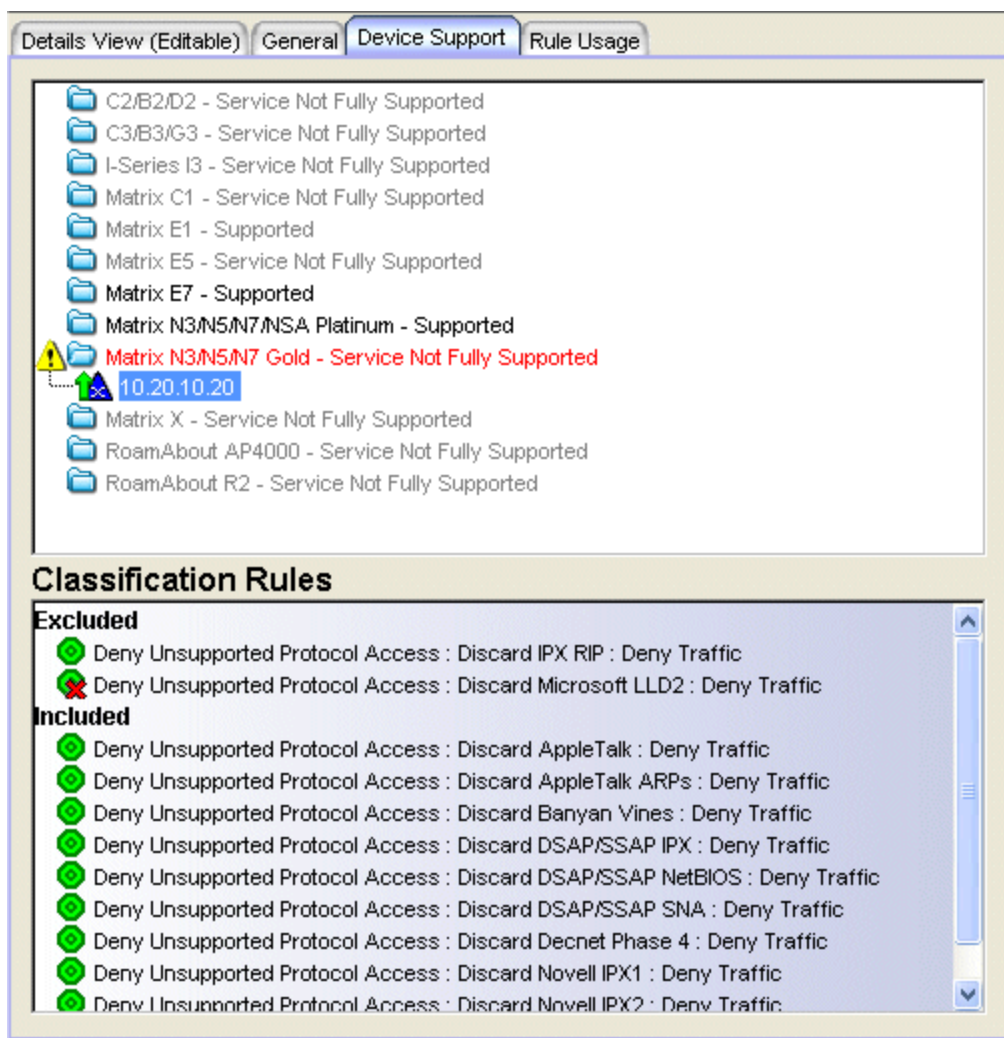
For information on related windows:

- [Enforce Preview Window](#)

## Device Support Tab (Service)

Use the service Device Support tab to view the classification rule information that will be written to your devices for the selected service, should you decide to [enforce](#) a role to which the service has been applied. The information is displayed according to device type, and is particularly useful if you have devices that only support certain aspects of policy management.

To access this tab, select a service in the left-panel Services tab, then select the Device Support tab in the right panel.



The screenshot displays the 'Device Support' tab in a network management interface. The interface has four tabs: 'Details View (Editable)', 'General', 'Device Support', and 'Rule Usage'. The 'Device Support' tab is active, showing a list of devices and their support status for a selected service. The devices listed are:

- C2/B2/D2 - Service Not Fully Supported
- C3/B3/G3 - Service Not Fully Supported
- I-Series I3 - Service Not Fully Supported
- Matrix C1 - Service Not Fully Supported
- Matrix E1 - Supported
- Matrix E5 - Service Not Fully Supported
- Matrix E7 - Supported
- Matrix N3/N5/N7/NSA Platinum - Supported
- Matrix N3/N5/N7 Gold - Service Not Fully Supported (highlighted with a warning icon)
- 10.20.10.20 (highlighted with a blue selection bar)
- Matrix X - Service Not Fully Supported
- RoamAbout AP4000 - Service Not Fully Supported
- RoamAbout R2 - Service Not Fully Supported


Below the device list, there is a 'Classification Rules' section. It is divided into 'Excluded' and 'Included' rules. The 'Excluded' rules are:

- Deny Unsupported Protocol Access : Discard IPX RIP : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard Microsoft LLD2 : Deny Traffic (red X icon)

The 'Included' rules are:

- Deny Unsupported Protocol Access : Discard AppleTalk : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard AppleTalk ARPs : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard Banyan Vines : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard DSAP/SSAP IPX : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard DSAP/SSAP NetBIOS : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard DSAP/SSAP SNA : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard Decnet Phase 4 : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard Novell IPX1 : Deny Traffic (green circle icon)
- Deny Unsupported Protocol Access : Discard Novell IPX2 : Deny Traffic (green circle icon)

## Top Panel

This section displays folders for different device types. Expand the folders to see your network devices and device groups organized according to device type. If the domain does not include any devices of a specific device type, that device type folder is displayed in gray. For those device types that are included in the domain, the device type folders are displayed in black when the service is fully supported, and red when it is not fully supported. In addition, the  icon alerts you that there are certain rules that will not be written to this device type if you enforce, that you might want to investigate.

Select a specific device type to display the classification rules that will and/or will not be written to those devices when you enforce a role to which the selected service has been applied.

## Classification Rules Area

Based on the device type selected in the top panel, this section displays the classifications rules that will be included or excluded for the selected service, should you decide to enforce a role to which the service has been applied.


---

**TIP:** Double-clicking a rule in this table opens the rule's General tab, where you can easily edit a rule's parameters. This is particularly useful for editing unsupported rules.

---

### Excluded

Lists any unsupported classification rules that have been applied to the selected service. These rules will not be included when the associated roles are written to the devices.

**NOTE:** Disabled rules  are always listed as Excluded.

---

### Included

Lists any supported classification rules that have been applied to the selected service. These rules will be included when the associated roles are written to the devices.

---

**NOTE:** On N-Series Platinum devices, range classification rules are achieved through applying subnet masks to values. As such, in order to achieve a user-specified range, the device may need multiple rules with subnets applied to encompass that range. So, although the user created only one rule with a range, this list may show multiple instances of that rule with the name of the rule followed by the portion of the over-all range it applies to.

---

## Related Information

For information on related concepts:

- [Enforcing](#)

For information on related windows:

- [Enforce Preview Window](#)

## General Tabs

---

A General tab is available in the right panel of the Policy Manager main window for many items selected in the left-panel tab. It provides general properties information about the selected item.

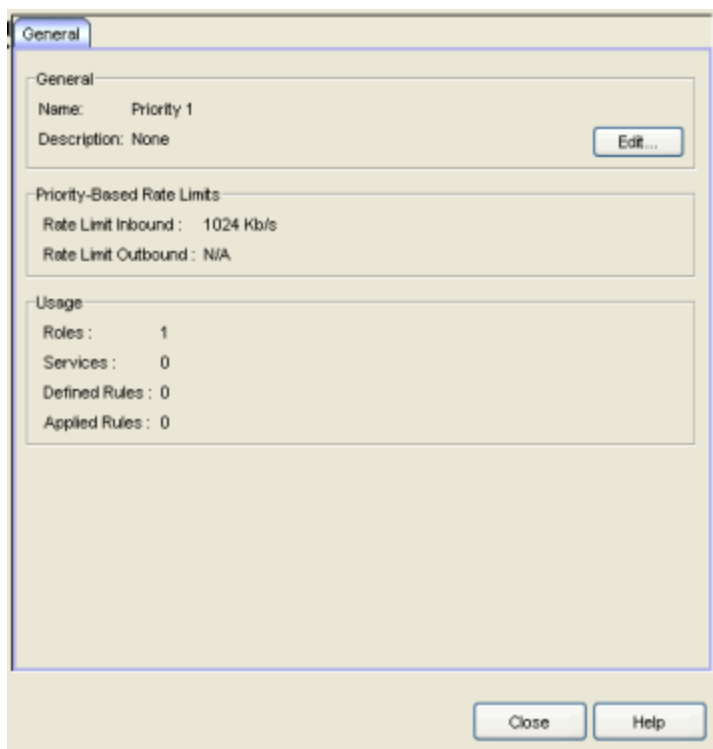
Help topics for the right-panel General tabs are named to reflect the item selected in the left-panel tree. For example, the Help topic for the General tab with a device selected in the left panel is named General Tab (Device). For more complete information on the different General tabs, expand the General Tabs section and select the desired tab.

## General Tab (802.1p Priority)

---

The 802.1p priority General tab provides information about the number of roles, services, and rules associated with the selected 802.1p priority, as well as information about any priority-based rate limits associated with the priority. It also lets you add or modify the priority's description.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select an 802.1p Priority in the tree, and the General tab will display in the right panel.



### Name

Name of the selected 802.1p priority.

### Description

Use the **Edit** button to open a window where you can add or modify a description for the priority.

### *Priority-Based Rate Limits*

This section provides information about any priority-based rate limits associated with the priority. See [How to Define Priority-Based Rate Limits](#) for more information.

#### **Rate Limit Inbound**

The priority-based inbound rate limit associated with the priority, if any. Otherwise, N/A. The rate limit sets the highest rate of speed at which traffic can enter a port before packets will be dropped.

#### **Rate Limit Outbound**

The priority-based outbound rate limit associated with the priority, if any. Otherwise, N/A. The rate limit sets the highest rate of speed at which traffic can exit a port before packets will be dropped.

### *Usage*

This section provides information about the number of roles, services, and rules associated with the 802.1p priority.

#### **Roles**

Number of roles associated with the 802.1p priority.

#### **Services**

Number of services associated with the 802.1p priority.

#### **Defined Rules**

Total number of rules utilizing this 802.1p priority. This includes rules that are enabled and are part of at least one role (applied rules), as well as rules not yet assigned to any roles.

#### **Applied Rules**

Number of rules utilizing this 802.1p priority that are enabled and are part of at least one role.

---

### **Related Information**

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)



## General Tab (Class of Service)

---

This tab lets you view and configure the components of a class of service (CoS). See below for a description of each section. For more information, see [How to Create a Class of Service](#).

Once you have created and defined a class of service, you can then apply it as a classification rule action, as part of the definition of an automated service, or as a role default. For more information, see [Getting Started with Class of Service](#).

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a class of service in the tree, and the General tab will display in the right panel.

---

**NOTE:** The actual columns that appear under Rate Limiting/Rate Shaping tab might vary based on the Port Details View and SNMP options settings on the [Policy Manager Options Window](#).

---

**General**

General

Name: RTP/Voice/Video

Description: None Edit...

Transmit Queue: Q3 (8Q) Edit...

802.1p Priority: Priority 6 (Legacy Devices) Priority-Based Rate: Inbound: N/A Outbound: N/A

ToS/DSCP Marking: 0x  DSCP: N/A Select... Mask: 0x ff

Drop Precedence: None

Rate Limiting / Rate Shaping

IRL Port Groups: Default

Inbound Rate Limits:

ORL Port Groups: Default

Outbound Rate Limits:

TxQ Port Groups: Default

TxQ Rate Shapers (Out):

Note: Flood Control is en/disabled per COS, but specified rates for a FC port group are shared by all CoS using FC.

Flood Ctrl Port Groups: Default

FC - Unicast Unknown: Disabled

FC - Multicast: Disabled

FC - Broadcast: Disabled

IRL (User) Port Grps: Default

In (User) Rate Limits:

ORL (User) Port Grps: Default

Out (User) Rate Limits:

IRL Index: -1 ... | ORL Index: -1 ... | TxQ Index: 6 ... | IUB Index: -1 ... | OUB Index: -1 ...

## General

### Name

Name of the selected class of service.

### Description

Use the **Edit** button to open a window where you can add or modify a description for the class of service.

### Transmit Queue

This field displays the transmit queue associated with the class of service for each port type. Use the **Edit** button to display a menu where you can

select a new transmit queue, if desired.

### 802.1p Priority

The 802.1p priority associated with the class of service, if any. The checkbox lets you enable or disable the priority, and the drop-down list lets you choose a different 802.1p priority, if desired. If the 802.1p priority is associated with a particular inbound and/or outbound [priority-based rate limit](#), that rate limit information will be displayed to the right. This field will be grayed out for the eight static classes of service provided by Policy Manager (Priority 0-7), because the 802.1p priority cannot be disabled or changed.

### ToS/DSCP Marking

Some IP rules allow a ToS/DSCP value to be written to the ToS/DSCP field in the IP header of incoming packets. This checkbox lets you enable or disable the IP ToS (Type of Service) or DSCP (Diffserv Codepoint) rewrite value associated with this class of service. See [ToS/DSCP Rewrite](#) and [ToS/DSCP Value Definition Chart](#) for more information.

- **Value** - The IP type of service value is an 8-bit hexadecimal number between 0 and FF (see [IP Type of Service](#) for more information). You can either enter this value in the **0x** text box, or click **Select** to open the [ToS/DSCP Configuration window](#), where you can automatically configure a ToS (Type of Service) or DSCP (Diffserv Codepoint) value.
- **Mask** - The ToS mask controls which bits in the ToS/DSCP field of incoming packets will be overwritten.

### Drop Precedence

The Drop Precedence option is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence will dictate the internal priority (within the MAC chip) that will be used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.

## *Rate Limiting/Rate Shaping*

This section displays the inbound/outbound rate limits (IRL/ORL) and the outbound transmit queue (TxQ) rate shapers that are configured for the Default port groups associated with the class of service. If you have created additional port groups, the information will be displayed for those groups as well.

With port rate limits, all traffic assigned to this class of service on a given port will share bandwidth specified by the rate limit. Rate shaping paces the rate at which traffic is transmitted out of the transmit queue. You can add or change a rate limit or a rate shaper by double-clicking on the area below a port group name.

If you have ExtremeWireless Wireless Controllers (Release 8.01.xx or higher) on your network, you will also see the IRL and ORL user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available on wireless controllers.

For more information, see [Advanced Rate Limiting by Port Type](#) and [How to Configure Transmit Queues](#).

### **Index Numbers**

At the bottom of the tab there is a section for configuring the rate limit and transmit queue index numbers associated with this class of service. These index numbers are used to map the class of service to the actual rate limits and transmit queue configuration on the device.

Typically, each class of service uses a different index number. Policy Manager automatically assigns these index numbers when you configure a class of services's rate limits and transmit queue shapers. An index number of "-1" indicates that no mappings are associated with the class of service.

All CoS using the same index will use the same rate limit and rate shaping assignments, and thus all traffic using those CoS will share the bandwidth.

### **IRL/ORL Index (Inbound/Outbound Rate Limits Index)**

The inbound/outbound port rate limit index associated with the class of service. Index numbers map logical rate limit indexes to the actual physical rate limits you have created in Policy Manager. Click the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings will apply for this

---

CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

### **TxQ Index (Transmit Queue Index)**

The transmit queue index associated with the class of service. Index numbers map logical transmit queue indexes on the ports to the actual physical transmit queues you have configured in Policy Manager. If you have selected an 802.1p priority for this class of service, a default transmit queue index is automatically specified based on the selected priority. You can use the default index or change it according to your own transmit queue configuration. Click the button to open the Transmit Queues selection view window, which lists all the possible transmit queues, organized by index number for each existing port type and group. Selecting an index automatically includes all the transmit queues configured for that index number.

### **IUB/OUB Index (Inbound/Outbound User-Based Rates Index)**

If you have ExtremeWireless Wireless Controllers (Release 8.01.xx or higher) on your network, you will also see the inbound/outbound user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for these wireless controllers. Click the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings will apply for this CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

### **Flood Ctrl Port Groups**

CoS-based flood control is a form of rate limiting that prevents configured ports from being disrupted by a traffic storm, by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unknown-unicast, broadcast, or multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

---

**NOTE:** By default, Flood Control is not managed by Policy Manager. To manage flood control configuration on devices in a domain, it can be enabled via the Domain Managed CoS Components drop-down menu by selecting All CoS Components or by selecting Flood Control.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

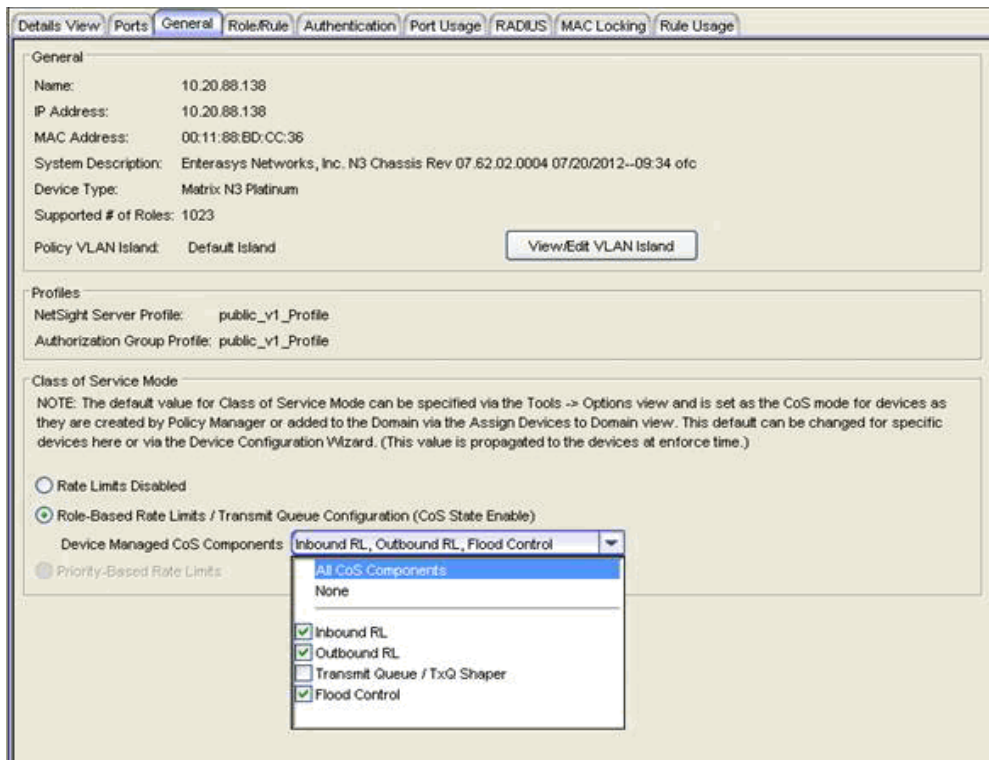
- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)

## General Tab (Device)

The device General tab provides identification information for the selected device. To access this tab, select a device on the left panel's Network Elements tab and click the General tab in the right panel.



### *General*

#### **Name**

Name of the device, or its IP address, if it does not have a name.

#### **IP Address**

IP address of the device.

#### **MAC Address**

Media access connection (hardware) address of the device.

#### **System Description**

Description of the device, including its manufacturer, model number and firmware revision number.

**Device Type**

Indicates the type of device. Certain devices may be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

**Supported # of Roles**

The number of roles supported by this device.

**Policy VLAN Island**

[Policy VLAN Island](#) with which the device is associated. This field appears only when the Policy VLAN Islands feature is enabled.

**View/Edit VLAN Island Button**

Opens the [Island Topology tab](#) for the Policy VLAN Island selected. From there you can access the other tabs for the VLAN island, and make changes if required.

*Profiles*

This section displays the profiles assigned to the device via the Profile/Device Mapping tab in the Authorization/Device Access window.

**NetSight Server Profile**

The profile assigned to the device for the NetSight Administrator group. The Read Credential of this profile is used to determine contact status for this device.

**Authorization Group Profile**

The profile assigned to the user's Authorization Group. The credentials of this profile define the user's access privileges for SNMP communication with the device.

*Class of Service Mode*

Policy Manager supports two modes of class of service, with each mode providing a different rate limit functionality:

- Role-Based Rate Limits and Transmit Queue Configuration - These rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the class of service.
- Priority-Based Rate Limits - Priority-based rate limits are used primarily by legacy devices. These rate limits are associated with one or more 802.1p



priorities, and are implemented based on the 802.1p priority assigned to a data packet appearing on a port.

---

**NOTE:** A default value for Class of Service Mode can be specified via the Tools > Options view. The default value is set as the CoS mode for devices as they are created by Policy Manager or added to the domain. The CoS mode settings that you set here for this specific device will override the default value set in the Options.

---

Select the class of service mode or select the option to disable rate limits on the device. If a mode is not supported on the device it will be grayed out. See [Getting Started with Class of Service](#) for more information on the two modes. You must Enforce to write these changes to the device.

### Rate Limits Disabled

Select this option if you want rate limits disabled on the device. This means that any priority-based rate limits will not be written to the device on enforce, and any role-based rate limits will not be included in roles written to the device on enforce.

### Role-Based Rate Limits/Transmit Queue Configuration (CoS State Enable)

Select this mode if you want to configure role-based rate limits and transmit queues on this device. See [Defining Role-Based Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.

### Device Managed CoS Components

Select CoS components (Inbound IRL, Outbound IRL, Transmit Queue/TxQ Shaper, or Flood Control) that are enabled at the domain level, but will be disabled for this device. The components selected here will be ignored during Enforce/Verify operations.

### Priority-Based Rate Limits

Select this mode if you want to configure priority-based rate limits on this device. Priority-based rate limits add to the amount of time it takes to enforce and verify roles. Once you've created your rate limits and enforced them, you may want to disable rate limits on the device so that it takes less time to enforce. See [Defining Priority-Based Rate Limits](#) for more information.

---

## Related Information

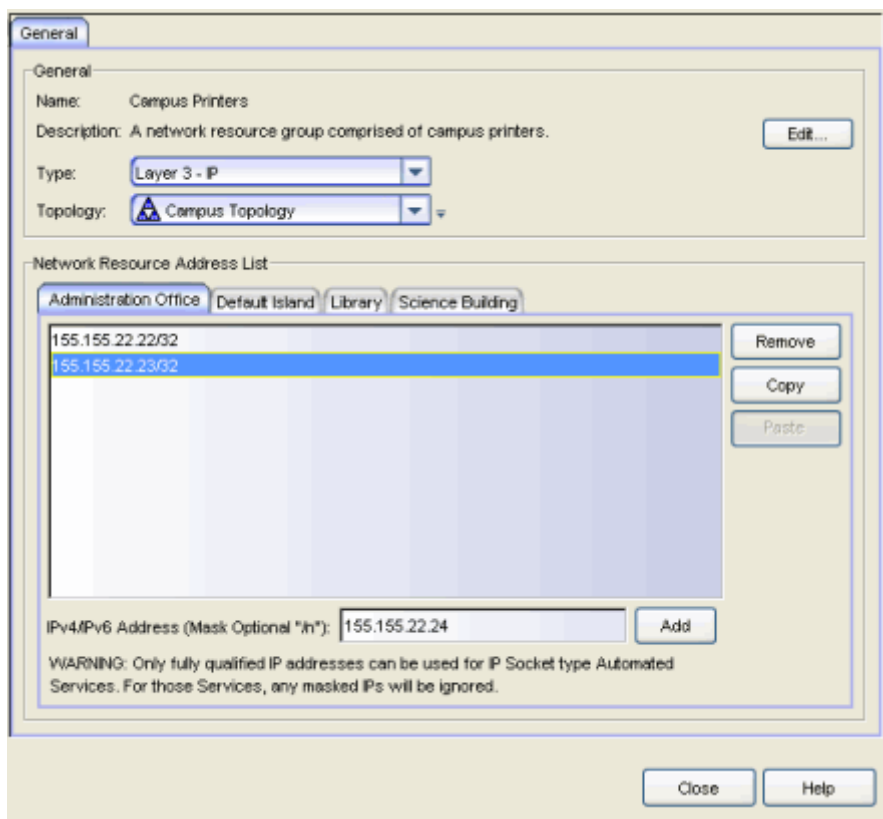
For information on related windows:

- [Authentication Tab \(Device\)](#)
- [Details View \(Device\)](#)
- [RADIUS Tab \(Device\)](#)

## General Tab (Network Resource Group)

This tab lets you configure a network resource group, which is a group of network resource devices that can be associated with an [Automated service](#). You configure the group by selecting a network resource type (MAC or IP) and [typology](#), and then creating a list of MAC or IP addresses for the resources that are part of the group. Once a network resource group has been defined, you can associate it with the desired Automated service (see [How to Create a Service](#) for more information).

To access this tab, select a network resource group in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu).



### Name

Name of the network resource group selected in the left panel.

### Description


Use the **Edit** button to open a window where you can add or modify a description for the network resource group.

## Type

Select the network resource type:

- Layer 2 MAC - Define a group of network resource MAC addresses.
- Layer 3 IP - Define a group of network resource IP addresses.

## Topology

Use this drop-down menu to select a [network resource topology](#) for this group. Use the configuration menu button  on the right to add a new topology or edit an existing topology.

## Network Resource IP Address List

For each topology island included in the selected topology, you will see a tab that lists the resources for that specific island. Use the address field (MAC or IP, depending on the selected type) to add a new resource to the list. Use the Copy and Paste buttons to copy a resource address from one island and paste it into another island.

---

## Related Information

For information on related tasks:

- [How to Create a Network Resource Group](#)
- [How to Create a Service](#)

## General Tab (Rate Limit)

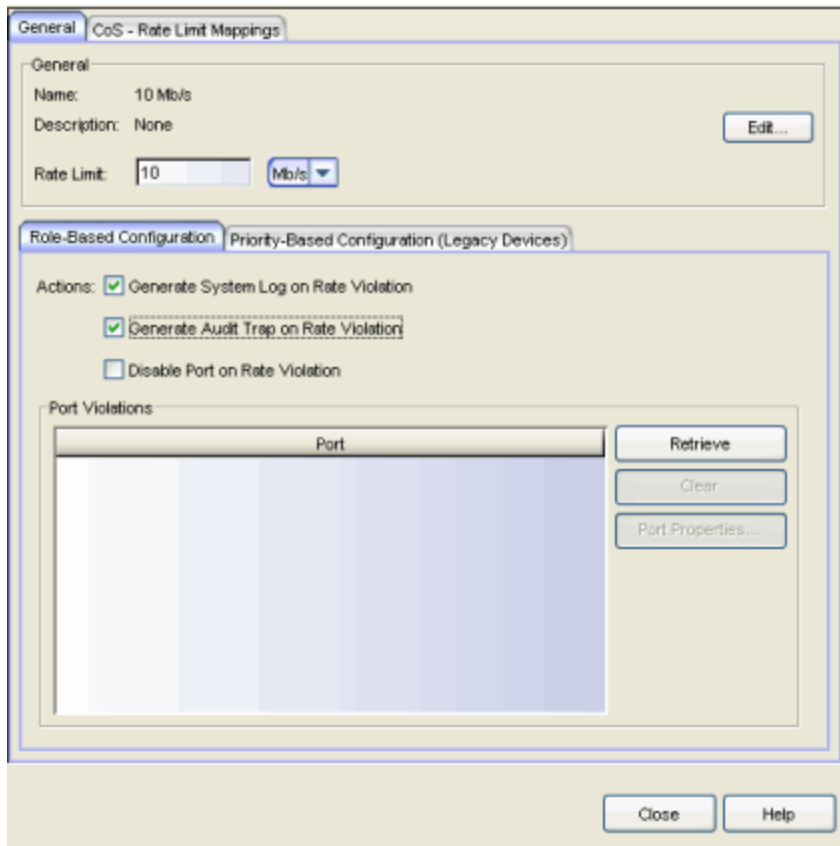
---

This tab lets you view and configure the parameters for a rate limit. Rate limits are components of a Policy Manager class of service, and are used to control the transmit rate at which traffic enters and exits ports in your network.

Policy Manager uses Role-Based rate limits that are tied directly to roles and rules, and are written to a device when the role/rule is enforced. Policy Manager also supports Priority-Based rate limits for use with legacy devices. (Refer to the NetSight Firmware Support tables to determine which type of rate limit a specific device/firmware supports.) Use the two sub-tabs to configure role-based and (if applicable) priority-based parameters for the rate limit.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a rate limit in the tree, and the General tab will display in the right panel.

If you make a change on this tab, you need to enforce in order for it to take effect.



### Name

Name of the selected rate limit.

### Description

Use the **Edit** button to open a window where you can enter or modify a description of the selected rate limit.

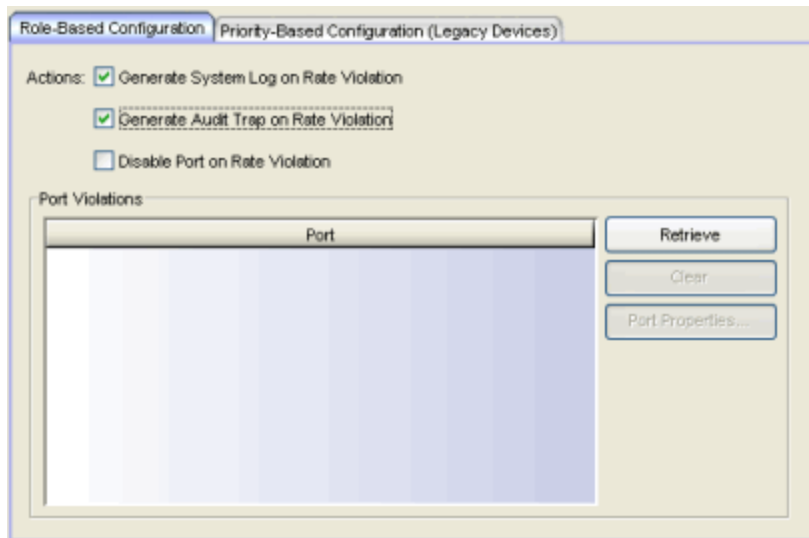
### Rate Limit

Specify the highest transmission rate at which traffic can enter or exit a port before packets will be rate limited:

- % - A percentage of the total bandwidth available (not available for priority-based rate limits)
- PPS - Packets per second (not available for priority-based rate limits)
- Kb/s - Kilobits per second
- Mb/s - Megabits per second
- Gb/s - Gigabits per second

## Role-Based Configuration Tab

Use this subtab to configure the actions for a [role-based rate limit](#) and view a list of ports where the rate limit has been exceeded.



### Actions

Select the action type(s) you would like this rate limit to use:

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

---

**NOTE:** N-Series Gold devices do not support rate limit notification.

---

### Port Violations Table

This table lists the ports where the rate limit has been exceeded. It displays the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Retrieve Button

Retrieves the most recent information about ports in violation.

### Clear Button

Clears the violations table. If port traffic continues to exceed the rate limit, ports will reappear in the table. Any ports disabled due to the rate violation

will be re-enabled.

### Port Properties Button

Select a port in the table and click this button to access the port's General tab where you can view and edit port information.

### Priority-Based Configuration Tab

Use this tab to configure parameters for a [priority-based rate limit](#). Priority-based rate limits are used primarily by legacy devices.

The screenshot shows the 'Priority-Based Configuration (Legacy Devices)' tab. At the top, there are two tabs: 'Role-Based Configuration' and 'Priority-Based Configuration (Legacy Devices)'. Below the tabs, there are several sections:

- Direction:** Radio buttons for 'Inbound' (selected) and 'Outbound'.
- Priority-Based Precedence:** A dropdown menu showing '3' and an 'Edit' button.
- 802.1p Priorities:** A row of eight checkboxes labeled 0 through 7. Priority 4 is checked, and priorities 0, 1, 2, 3, 5, 6, and 7 are grayed out.
- C2/B2 10/100 Priority:** Two checkboxes: 'Low (0-3)' and 'High (4-7)'. Both are currently unchecked.
- Priority-Based Rate Lim:** A text area with the text: 'affect all ports other than explicitly excluded, regardless of the use of roles on those ports'.
- Exclusion:** A section with the text 'Select any network elements that should be explicitly excluded from being rate limited.' Below this is a large empty table area with an 'Edit...' button and a 'Remove' button.

### Direction

Select Inbound or Outbound, depending on whether the rate limit is for inbound or outbound traffic. In order to control traffic inbound and outbound on the same port, two rate limits must be configured (one inbound and one outbound). Inbound rate limiting takes place after a frame has been classified into one of the eight priorities. Outbound rate limiting takes place just before a frame is queued for transmission.

### Precedence

The order in which priority-based rate limits will be written to devices that support them. Click **Edit** to open the [Precedence tab](#), where you can change the order in which rate limits will be applied.

### 802.1p Priorities

Select the 802.1p priority or priorities with which the rate limit will be associated. Each 802.1p priority can have only one inbound and one outbound rate limit; therefore, if a priority is already being utilized for the selected direction, it is grayed out.



### C2/B2 10/100 Priority

C2/B2 10/100 ports support two rate limits (inbound only). If you are creating a rate limit to be used on C2/B2 10/100 ports, select either Low to associate the rate limit with priorities 0-3 or High to associate the rate limit with priorities 4-7. You can select both Low and High if you want to associate the rate limit with priorities 0-7. If the Low or High priority is already being utilized for another rate limit, it will be grayed out. Because C2/B2 10/100 ports only support inbound rate limits, this section will be grayed out if you have selected Outbound for your rate limit [Direction](#). C2/B2 Gigabit ports support eight rate limits (inbound only); for those ports, select the [802.1p priorities](#) as you would for other ports.

### Exclusion

Specify the network elements to which this rate limit will *not* apply. For example, rate limiting is most often used for edge devices; therefore, you might want to exclude a device group or port group containing non-edge devices or ports. Click **Edit** to open the [Add/Remove Network Elements window](#) where you can select network elements to exclude from the rate limit. To remove a network element from the exclusion list, select it and click **Remove**.

---

### Related Information

For information on related concepts:

- [Rate Limits](#)
- [Priority-Based Rate Limits](#)

For information on related tasks:

- [How to Define Rate Limits](#)
- [How to Define Priority-Based Rate Limits](#)

For information on related windows:


- [Precedence Tab](#)

## General Tab (Role)

---

The [role](#) General tab lets you assign default actions for a role that will be applied to traffic not identified specifically by the set of access services contained in the role. You can also use this tab to enable TCI Overwrite functionality for the role, and enter or edit the description of the role.

The Services section displays a list of the services and service groups associated with the selected role, and provides buttons for adding and removing services, creating a new service, viewing and editing a service or service group, and showing conflicting rules.

If you have selected the Quarantine role or any role that has been specified as a quarantine action for one or more rules, you will see a Warning at the top of the tab reminding you that the role should be configured to be highly restrictive and to use caution when adding services to the role. Click the  button to view a list of the services currently using the Quarantine role.

To access this tab, select a role in the left panel's Roles tab, then select the General tab in the right panel. Any additions or changes you make to this tab must be [enforced](#) in order to take effect

The screenshot shows the configuration interface for a role named "Enterprise User". The "General" tab is selected, and the "Name" field contains "Enterprise User". The "Description" field contains a long text describing the role's equivalence to the Enterprise Access role. The "TCI Overwrite" dropdown is set to "Disabled".

**Default Actions:**

- Access Control: Permit Traffic
- Class of Service: Network Control [Static]
- System Log: Disabled
- Audit Trap: Disabled
- Disable Port: Disabled
- Traffic Mirror: Appliance Ports

**Wireless Controller Only:**

- Wireless Default Access Control: Contain to VLAN
- Contain to VLAN: 1 [DEFAULT VLAN]
- Discard Unmatched Traffic (Pre-8.3x FW & 8.21 Compatibility Mode Only)

**Services:**

Name	Also Used By Roles
Acceptable Use Policy	Enterprise Access
Application Provisioning - NAC	Assessing, Deny Access, Enterprise Access, Guest Access,
Authenticated Supplemental Privileges	Notification

Buttons on the right side of the Services section include: Add/Remove Services..., Create Service..., View/Edit Service/Grp, and Show Conflicting Rules...

## Name

Name of the selected role.

## Description

Use the **Edit** button to open a window where you can enter or modify a description of the role.

## TCI Overwrite

Enable or disable TCI Overwrite functionality for the role. Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this role or any of its rules to overwrite the VLAN or class of service (CoS) tag in a received packet if that packet has already been tagged with VLAN or CoS information. If TCI Overwrite is not enabled, tagged packets will egress using the TCI data they already contain. You can also enable TCI Overwrite on a per-port basis in the [Port Properties General Tab](#), as well as on a per-rule basis in the [Rule General Tab](#).

## Default Actions


Default actions for a role are applied to traffic not identified specifically by the set of access services contained in the role.

### Access Control

Use the drop-down list to choose a default access control (VLAN) for the role. You can select:

- None - No default access control specified.
- Permit Traffic - Allows traffic to be forwarded with the port's assigned VID.
- Deny Traffic - Traffic will be automatically discarded.
- Contain To VLAN - This option contains traffic to the VLAN specified. Use the drop-down list to the right to select the desired VLAN.

### Class of Service

Use the drop-down list to choose a default class of service (priority) for the role, create a new class of service, or select None if no class of service is desired. The drop-down list displays all of the classes of service for the current domain and also allows you to edit a class of service using the Edit button .

### System Log

When this option is enabled, a syslog message is generated as long as no matching rules specify that sending a syslog message is prohibited (that is, the rule's system log action is set to "Prohibited" on the [Rule General tab](#)). When the option is disabled, the system log setting is ignored.

### Audit Trap


When this option is enabled, an audit trap is generated as long no matching rules specify that sending an audit trap is prohibited (that is, the rule's audit trap action is set to "Prohibited" on the [Rule General tab](#)). When the option is disabled, the audit trap setting is ignored.

### Disable Port

When this option is enabled, the port is disabled as long no matching rules specify that disabling the port is prohibited (that is, the rule's disable port action is set to "Prohibited" on the [Rule General tab](#)). Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#). When the option is disabled, the disable port setting is ignored.

## Traffic Mirror

Use the drop-down list to specify port groups where [mirrored traffic](#) will be sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.

To the right of the drop-down list is an option to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to a Application Analytics appliance. The Application Analytics appliance only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and appliance. By default this number is set to 10, but can be changed by clicking on the Edit button .

**NOTE:** The value you set is used by all mirror actions in use in the current domain.

## Services

### Name

Lists the names of the services and service groups (local and global) associated with the selected role.

### Also Used By Roles

List the other roles using this service. If the service is a global service, the domain name is also displayed if the role is in a different domain.

### Add/Remove Services Button

Opens the role [Add/Remove Services window](#), where you can add and remove services and service groups to and from any of the existing roles.

### Create Service Button

Opens the [Service Wizard](#), where you can create a new service.

### View/Edit Service/Grp Button

Select a service or service group in the table and click this button to open the left-panel Services tab. The appropriate service or service group will be selected and you can access its right-panel tabs.

### Show Conflicting Rules Button

If the rules in a Global service conflict with the rules in a Local service, the Name column will display a message indicating that the global rules will be overridden by the local rules. Click on the **Show Conflicting Rules** button to open a window that displays the rule conflicts and shows specifically which rules will be used and which will be overridden. For more information, see [Conflict Checking](#).

## **Related Information**

For information on related tasks:

- [How to Create a Role](#)
- [How to Create a Class of Service](#)

## General Tab (Roles Folder)

---

This tab provides a place for you to enter a description of the domain's roles. To access this tab, select the Roles folder in the left panel's Roles tab and click the General tab in the right panel.



---

## Related Information

For information on related windows:

- [Details View Tab \(Roles Folder\)](#)

## General Tab (Rule)

The rule General tab displays general information about the rule selected in the left-panel Services tab and enables you to change it. In addition, you can view and change the Traffic Description and Actions associated with the rule. Traffic Description identifies the type of traffic to which the rule pertains. Actions apply class of service, access control, and/or accounting and security behavior to packets matching the rule.

Any additions or changes you make to this tab must be [enforced](#) in order to take effect. If you modify an enabled rule's actions, Policy Manager checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See [Conflict Checking](#) for more information.

The screenshot shows the 'General' tab for a rule named 'Discard UDP Src 53 - DNS Imposters'. The interface is divided into three main sections: General, Traffic Description, and Actions.

- General:** Name: Discard UDP Src 53 - DNS Imposters; Description: Hackers/crackers may be attempting to do zone transfers (TCP), to spoof DNS (UDP), or even hide other traffic since port 53 is frequently neither filtered nor logged by firewalls. An important thing to note is that you will frequently see port 53 used as the source UDP port. Stateless firewalls frequently...; Rule Status: Enabled; Rule Type: All Devices; TCI Overwrite: Disabled.
- Traffic Description:** Traffic Description Type: IP UDP Port Source; Traffic Description Value: DNS.
- Actions:** Access Control: Deny Traffic; Class of Service: None; System Log: Disabled; Audit Trap: Disabled; Disable Port: Disabled; Traffic Mirror: App ID Appliance; Quarantine Role: Quarantine. A 'Contain to VLAN' dropdown is set to 'N/A'. A note states: 'Note: Syslog Server(s) may be configured via Console'. A checkbox for 'Mirror first 10 packets/flow' is checked. Another note states: 'Note: Requires Quarantine Auth status be enabled on devices & ports'.

### General Area

#### Name

Displays the name of the rule.



## Description

Use the **Edit** button to open a window where you can enter or modify a description of the rule.

## Rule Status

Lets you disable the rule, or enable it if it's already disabled. If the rule is disabled, it is unavailable for use by the current service, but can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is an alternative to deleting and recreating it. You can also disable/enable rules in the Rule Status window of the [Service Wizard](#) or [Classification Rule Wizard](#). The rule icon in the left panel displays a red X if the rule is disabled.

## Rule Type

Use the drop-down list to select the types of devices to which you wish this rule to apply when enforced. The recommended selection is All Devices, unless there is a specific need for a device-specific rule. If this need arises, the Rule Type feature allows services to be customized to contain rules specific to a device's type when support for a traffic description and/or action may not be available on all managed devices.

For device-specific rules, only those traffic descriptions that are supported on the device will be available when you define the rule's traffic description on this tab or in the [Classification Rule Wizard](#). For All Devices rules, all traffic descriptions are available; however, you must be aware that you cannot enforce the rule to a device which does not support it. The [Enforce Preview](#) window and the Device Support tabs for [roles](#), [services](#), and [rules](#) enable you to see what rules will and will not be written to the device.

## TCI Overwrite

Specify the TCI Overwrite functionality for the rule:

- **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

## *Traffic Description Area*

The Traffic Description area allows you to view and change the traffic description associated with a rule. The Traffic Description identifies the traffic classification type for the rule. Rules allow you to assign access control (VLAN membership) and/or class of service to network traffic depending on the traffic's classification type.

### **Traffic Description Type**

Displays the Classification Type selected for the rule.

### **Traffic Description Value**

Displays the values/parameters selected for the rule's Classification Type. See [Classification Types and their Parameters](#) for parameter information.

### **Remove Button**

Removes the traffic description from the rule.

### **Edit Button**

If a Traffic Description Type has been defined for the rule, clicking Edit opens the [Edit Rule window](#), where you can edit the parameters or values for the rule's classification type. If there is no Traffic Description type defined (None), clicking Edit opens the [Traffic Description Wizard](#) where you can define a Traffic Classification type and parameters for the rule.

## *Actions Area*

The Actions area allows you to view and change the actions associated with a rule. Actions apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

### **Access Control**

Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select **None** to disable access control for this rule.

- **Permit Traffic** - allows traffic to be forwarded with the port's assigned VID.
- **Deny Traffic** - traffic will be automatically discarded.
- **Contain to VLAN** - contains traffic to a specific VLAN. Use the drop-down list to select the desired VLAN.

## Class of Service

Use the drop-down list to select a class of service to associate with the rule. Policy Manager lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See [Getting Started with Class of Service](#) and [How to Create a Class of Service](#) for more information. Select **None** to disable class of service for this rule.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use the following three options to specify certain rule usage actions to take place when a "rule hit" is reported.

## System Log

Specify System Log functionality for the rule. Syslog receivers are configured in NetSight Console. Refer to the Help topic in the Console User Guide for more information.

- **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

## Audit Trap

Specify Audit Trap functionality for the rule:

- **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.


## Disable Port

Specify Disable Port functionality for the rule:

- **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
- **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

## Traffic Mirror

Specify [traffic mirroring](#) functionality for the rule:

- **Select port group(s)** - Use the drop-down list to specify the port groups where mirrored traffic will be sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection. To the right of the drop-down list is an option to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to a Application Analytics appliance. The Application Analytics appliance only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and appliance. By default this number is set to 10, but can be changed by clicking on the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.
- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

## Quarantine Role

Specify the [Quarantine Role](#) functionality for the rule:

- **Select Role** - Use the drop-down list to select the role that you want to assign as a Quarantine role. Specifying a role as a Quarantine role

turns the role's icon red, denoting its restrictive nature.

- **Disabled** - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
  - **Prohibited** - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.
- 

### Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [Using the Rule Tabs](#)

For information on related windows:

- [Device Support Tab \(Role\)](#)
- [Device Support Tab \(Rule\)](#)
- [Device Support Tab \(Service\)](#)

## General Tab (Service)

For Automated services, use the service General tab to define settings for the service. For Manual services, use this tab to enter a description of the service. For more information on services, see [How to Create a Service](#). To access this tab, select a service in the left-panel Services tab and click the General tab in the right panel. The General tab for an Automated service is shown below.

The screenshot shows the 'General' tab of a service configuration window. The window has three tabs: 'Details View', 'General', and 'Device Support'. The 'General' tab is active. The configuration is organized into several sections:

- General:** Name: SAP Servers; Description: None; TCI Overwrite: Disabled. An 'Edit...' button is located to the right of the Description field.
- Traffic Description:** Network Resource Type: Layer 3 - IP; Network Resources: SAP Servers; Rule Type: IP Address Bilateral.
- Actions:** Access Control: Permit Traffic; Class of Service: High Priority (802.1p: 7); System Log: Disabled; Audit Trap: Disabled; Disable Port: Disabled; Traffic Mirror: Disabled. A 'Contain to VLAN: N/A' dropdown is also present.

A note at the bottom right of the Actions section states: 'Note: Syslog Server(s) may be configured via Console'.

### Name

Name of the selected service.

### Description

Use the **Edit** button to open a window where you can enter or modify a description of the service.

## TCI Overwrite

Specify the TCI Overwrite functionality for the service:

- **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this service to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

## *Traffic Description Area*

Use this area to provide the specifications for an automated service. You will need to specify the network resource type and the network resources for the service. You will also need to specify the rule type. Some rule types require that you enter certain parameters and/or values. This section is not displayed for a Manual service.

### Network Resource Type

Select the network resource type (Layer 2 MAC or Layer 3 IP). This will determine the list of network resources available for selection for this service.

### Network Resources

Use the drop-down list to select the network resources to associate with the automated service. Use the configuration menu button to the right of the list to add a network resource or view and edit your network resources. For more information, see [How to Create a Network Resource](#).

### Rule Type

Select the type of rule you want to create for the network resources. Some rule types require that you enter certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information. Select and/or enter the required parameters.

## *Actions Area*

Use this area to define the access control and/or a class of service for the Automated service rule. This section is not displayed for a Manual service.

## Access Control

Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select **None** to disable access control for this rule.

- **Permit Traffic** - allows traffic to be forwarded with the port's assigned VID.
- **Deny Traffic** - traffic will be automatically discarded.
- **Contain to VLAN** - contains traffic to a specific VLAN. Use the drop-down list to select the desired VLAN. Use the configuration menu button to the right of the drop-down list to add or edit a VLAN.

## Class of Service

Use the drop-down list to select a class of service to associate with the service. Policy Manager lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See [Getting Started with Class of Service](#) and [How to Create a Class of Service](#) for more information. Select **None** to disable class of service for this rule. Use the configuration menu button to the right of the drop-down list to add or edit a Class of Service.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. The next three options allow you to specify certain rule usage actions to take place when a "rule hit" is reported.

## System Log

Specify System Log functionality for the rule:

- **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.



## Audit Trap

Specify Audit Trap functionality for the rule:

- **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

## Disable Port

Specify Disable Port functionality for the rule:

- **Enabled** - If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device [Role/Rule tab](#).
- **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

## Traffic Mirror

Specify [traffic mirroring](#) functionality for the rule:

- **Select port group(s)** - Use the drop-down list to select the port groups where mirrored traffic will be sent for monitoring and analysis. Use the configuration menu button to the right of the drop-down list and select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.
- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

## Related Information

For information on related tasks:

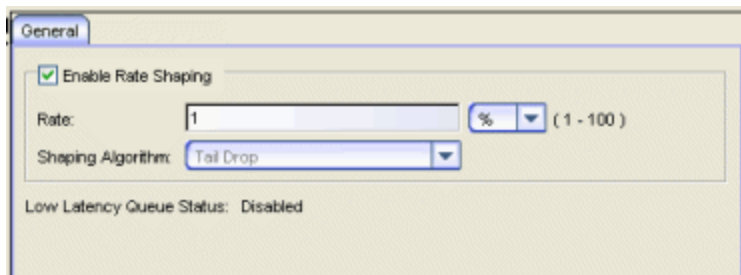
- [How to Create a Service](#)
- [How to Create a Network Resource](#)

## General Tab (Transmit Queue)

---

This tab lets you view and configure the rate shaping and low latency queue status settings for the selected transmit queue. Rate shaping paces the rate at which traffic is transmitted out of the transmit queue and sets the shaping algorithm which determines what will happen to traffic that exceeds the maximum amount of traffic the transmit queue can hold. Low latency status allows the queue to have a low transmit latency. This is typically used for traffic such as Voice over IP (VoIP). Not all transmit queues support the low latency setting.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Expand a transmit queue port group in the tree and select a transmit queue, then select the General tab in the right panel.



### *Enable Rate Shaping*

Rate shaping paces the rate at which traffic is transmitted out of the selected transmit queue. Rate shaping is disabled by default. Use the checkbox to enable rate shaping for the selected transmit queue.

---

**NOTE:** Matrix N-Series Gold devices do not support rate shaping.

---

### Rate

Specify the rate at which traffic will be transmitted out of the queue. The ranges for each rate are listed.

- % - A percentage of the total bandwidth available
- Kb/s - Kilobits per second

- Mb/s - Megabits per second
- Gb/s - Gigabits per second

### Shaping Algorithm

The shaping algorithm determines what will happen to traffic when the maximum amount of traffic the transmit queue can hold is exceeded. The algorithm is set by default to Tail Drop and the other options are not currently supported.

- Tail Drop - Discards the last entry in the queue in favor of new entries.
- Head Drop - Discards the first entry in the queue in favor of new entries.
- Random Early Discard - Discards queued packets randomly. This algorithm is used to encourage TCP end stations to back off their transmission rates when the transmit queues are overflowing.
- Weighted Random Early Discard - Verifies the priority of the packet before making a discard decision, and attempts to discard the lowest priority traffic first.

### *Low Latency Queue Status*

The Low Latency feature is disabled by default and is not currently supported. The feature would allow traffic assigned to this queue to have a low transmit latency. This is typically used for traffic such as Voice over IP (VoIP).

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

## General Tab (VLAN)

The VLAN General tab displays information about the VLAN selected in the left panel and lets you configure certain VLAN parameters. If you are using [VLAN to Role mapping](#) in your network, you can also use this tab to map the VLAN to a specific role. If you make a change on this tab, you need to enforce it using the **Enforce** button on the toolbar.

To view this tab, select a VLAN in the left panel of the Access Control Configuration window (available from the Policy Manager Edit menu).

General

General

Name: VoIP  
VLAN ID: 40

This VLAN is intended as a Discard VLAN only

Enable Dynamic Egress

Always write VLAN to device(s)

Tagged Packet VLAN to Role Mapping

NOTE: To forward traffic with the VLAN ID & CoS specified by the mapped Role, TCI Overwrite must be enabled. The Stackable devices support rewriting the CoS values but not the VLAN ID.

Device Level Mapping : Enterprise User Select

Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping

Port Level Mappings:

Port	Role
[10.20.77.33] Port fe.4.10	Notification
[10.20.77.33] Port fe.4.12	Notification

Add/Remove Mappings

Authentication Based VLAN (RFC3580) to Role Mapping

Mapped To Role: <None> Select

Close Help

### General

This area provides general information about the VLAN and allows you to configure the VLAN.

#### Name

Name of the VLAN selected in the left panel.

## VLAN ID

Unique number assigned to the VLAN, also called VID (for VLAN ID). This ID was either assigned by an administrator or assigned automatically by the system when the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

### This VLAN is intended as a Discard VLAN only

Select this checkbox if this VLAN is to be used to deny traffic. If it is to be used to contain traffic, leave the box unchecked.

### Dynamic Egress Enabled

Dynamically add all ports which use this VLAN to this VLAN's egress list. Dynamic Egress is enabled by default in Policy Manager. Leave disabled for discard VLANs. See [Dynamic Egress](#) for more information.

### Always write VLAN to device(s)

If the box is checked, the VLAN will be written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN will not be written to the device unless it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it allows you to configure that VLAN for Dynamic Egress. If the Default VLAN (VID=1) is selected in the left panel, this option is checked and cannot be edited, as the default VLAN is always on the device.

## *Tagged Packet VLAN to Role Mapping*

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see [VLAN to Role Mapping](#) in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

### **NOTE: TCI Overwrite Requirement**

-- Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingress with.  
-- If supported by the device, you can enable TCI Overwrite on a per-port basis in the [Port Properties window General tab](#), or for an individual role in the role's [General tab](#). The stackable devices support rewriting the CoS values but not the VLAN ID.

## Device Level Mapping

The role the VLAN is mapped to at the device level (all devices). To select a role, click **Select**, choose a role, and click **OK**.

### Select

Opens the role [Selection View](#), where you can choose a role to associate with the VLAN at the device level.

## Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping


Use this checkbox to specify that this VLAN to role mapping will be the primary mapping for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make this selection, there will be no device-level mapping for these devices.

## Port Level Mappings

This table lists any port-level Tagged Packet VLAN to Role Mappings that have been configured for this VLAN. Port-level mappings will override any device-level mapping.

---

**NOTES:** — You must have the Port Level Role Mappings feature enabled in Policy Manager for the mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored and any mappings listed here will be grayed out.

— Port-level mappings cannot be added or removed to or from frozen ports . You must clear the frozen state on a port in order to add or remove a mapping. Once you have created a mapping, you can freeze the port. The port-level mappings of the frozen port will still be enforced and verified.

---

## Add/Remove Mappings

Opens the [Add/Remove Mappings window](#) where you can add or remove port-level mappings. You can also configure port-level mappings using the [Mappings sub-tab](#) in the Port Properties General tab.

## *Authentication-Based VLAN to Role Mapping*

Authentication-Based VLAN to Role Mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. (For more information, see [VLAN to Role Mapping](#) in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to (at the device-level) and lets you configure a mapping, if desired.

**NOTE:** When configuring Authentication-Based VLAN to role mapping, you must enable RFC3580 VLAN Authorization on the device via the [device Authentication tab](#).

---

### Mapped to Role

The role the VLAN is mapped to. To select a role, click **Select**, choose a role, and click **OK**.

### Select

Opens the role [Selection View](#), where you can choose a role to associate with the VLAN.

---

## Related Information

For information on related concepts:

- [Dynamic Egress](#)
- [Policy VLAN Islands](#)

For information on related tasks:

- [How to Create a VLAN](#)
- [How to Create a Policy VLAN Island](#)



## Island Topology Tab (Policy VLAN Islands)

---

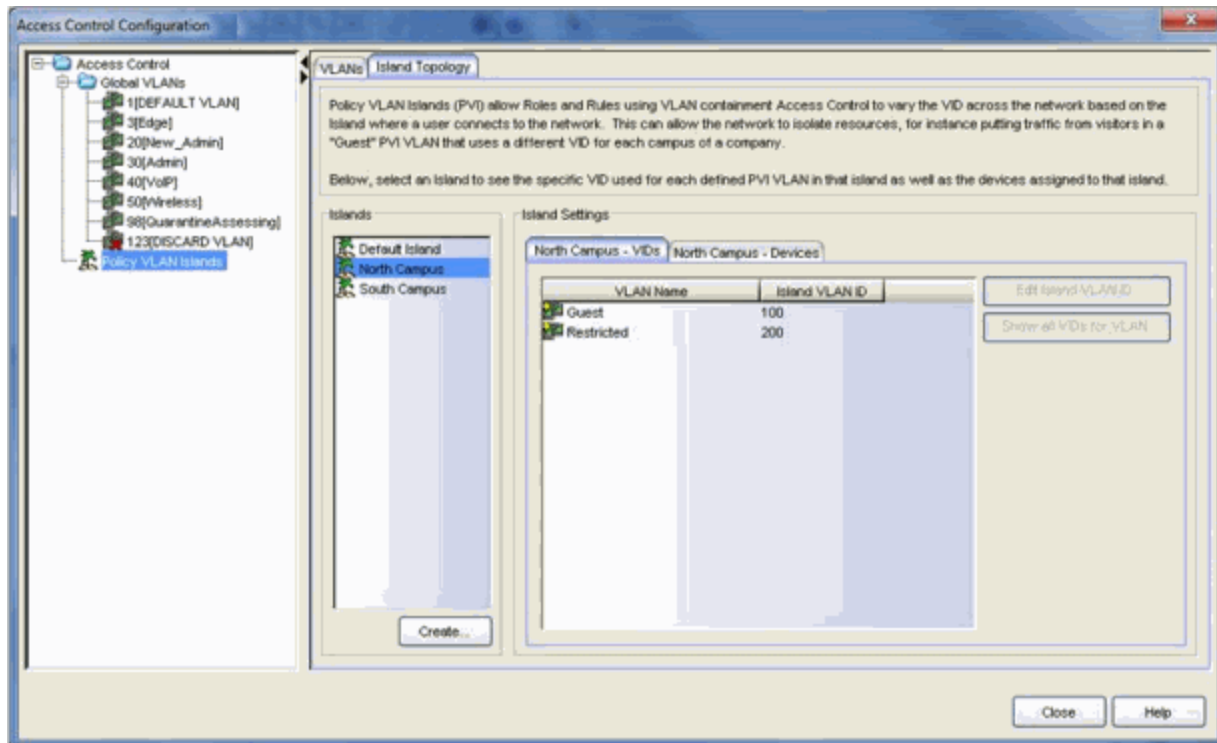
This tab displays a table of information about the [Policy VLAN Islands](#), which shows the VIDs used in the selected island for all defined PVI VLANs. To access this tab, select the Policy VLAN Islands node in the tree of the Access Control Configuration view, and select the Island Topology tab on the right panel.

The **Island Topology** tab provides two sub-tabs:

- [\(Island\) - VIDs Tab](#)
- [\(Island\) - Devices Tab](#)

### (Island) - VIDs Tab

This tab provides information on VIDs assigned to specific islands. When an island is selected, the VIDs tab shows all VIDs for the defined PVI VLANs that will be used for that island.



### Islands

Name of all defined PVI islands. Select an island to see the VIDs and devices associated with that Island, of the VLAN island in which the Island VLAN is being used.

### VLAN Name

Shows the defined PVI VLANs in the Domain. Unlike global VLANs, PVI VLANs are not created by Policy Manager during enforce. It is left to the user to configure these on the device(s) externally. Policy Manager will only associate the appropriate VIDs to the rules during enforce.

### Island VLAN ID

Shows the VID used for this PVI VLAN in this Island.

### Edit Island VLAN ID

Selecting an island in the table and clicking this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

### Show all VIDs for VLAN

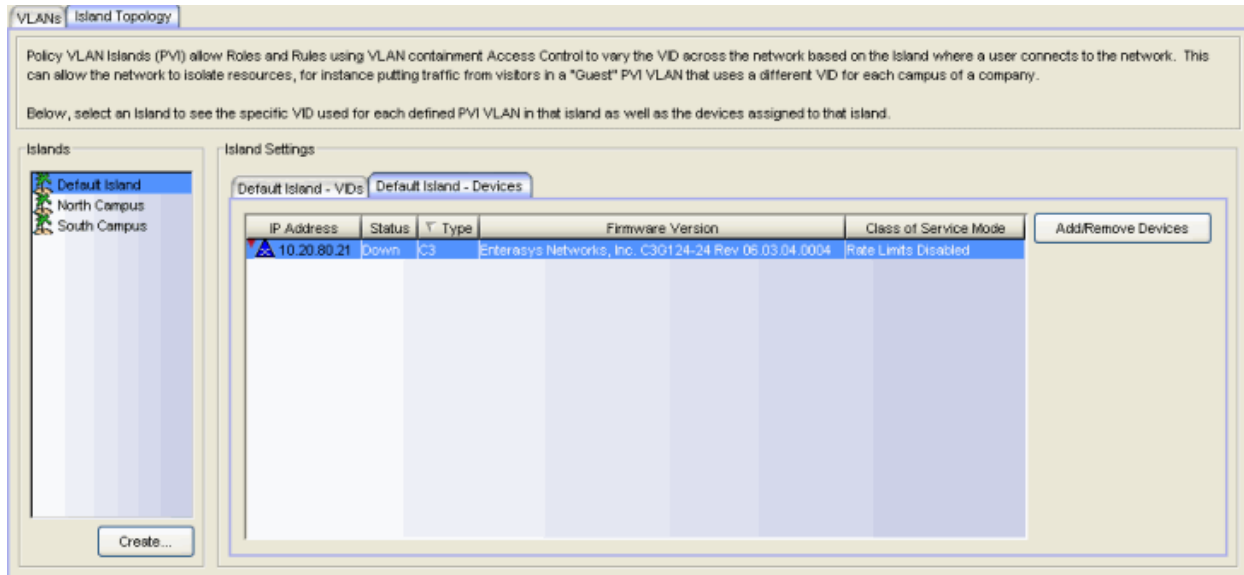
Selecting an island in the table and clicking this button opens the selected VLAN's [VLANs tab](#).

## Create

Opens the Create VLAN Island dialog. For more information, see [Creating a VLAN Island](#).

## (Island) - Devices Tab

This tab displays the devices that are part of a [Policy VLAN Island](#). To see a menu of options for a device in the table, right-click the device.



### IP Address

The device's IP address.

### Status

The device's current operational status.

### Type

Indicates the type of device.

### Firmware Version

Shows the current firmware revision for this device.

### Class of Service Mode

Indicates the Class of Service Mode.

### Add/Remove Devices

Opens a separate dialog to add/remove devices to specific Islands. For more information, see [Add/Remove Devices window](#).

## Create

Opens the Create VLAN Island dialog. For more information, see [Creating a VLAN Island](#).

---

## Related Information

For information on related concepts:

- [Policy VLAN Islands](#)
- [Network Resource Groups](#)

For information on related tasks:

- [How to Create a Policy VLAN Island](#)
- [How to Create a Network Resource Group](#)

## MAC Locking Tab (Device)

The device MAC Locking tab lets you enable the MAC Locking feature on devices that support it. You can also view and change a list of MAC addresses that are currently locked on the selected device. (Click the **Retrieve** button to display this information.) To access this tab, select a device that supports MAC Locking on the left-panel Network Elements tab, and click the MAC Locking tab in the right panel.

[MAC Locking](#) ensures that only a specific MAC address can access a port, and that traffic from any other MAC addresses will be discarded. In order for MAC Locking to take effect on a port, it must first be enabled at the device level. You can do this on this tab, or in the [Device Configuration wizard](#).

Details View | Ports | General | Role/Rule | Authentication | Port Usage | RADIUS | **MAC Locking** | Rule Usage

MAC Locking Status

MAC Locking :  Enabled  Disabled

Static MACs

Move all dynamic MACs with a Locking Cause of "First Arrival" to a statically locked MAC. Apply

Locked MAC Addresses

Device	Port IfName	Index	MAC Address	Locking Cause
12.22.70.30	fe.2.1	320	00:00:1D:2A:38:B1	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:2B:6B:89	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:2E:E1:9C	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:2E:E7:25	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:2F:1B:9B	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:4D:B1:89	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:4D:B3:75	Static
12.22.70.30	fe.2.1	320	00:00:1D:77:78:98	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:88:88:88	First Arrival
12.22.70.30	fe.2.1	320	00:00:1D:D0:45:4A	First Arrival
12.22.70.30	fe.2.1	320	00:01:F4:0A:29:BB	Static

Retrieve Add... Remove

### MAC Locking Status

Lets you enable or disable the MAC Locking feature on this device. If the device does not support the MAC locking feature, this option is grayed out.

### Static MACs

Click **Apply** to change all Dynamic Locked MAC addresses (with the [Locking Cause](#) of "First Arrival") to Static Locked MAC addresses. To ensure that all Dynamic Locked MAC addresses are changed to Static, make sure that the **Maximum Number of Static Locked MAC Addresses** is set to a large enough value in the [Port Properties MAC Locking Tab](#).

## Locked MAC Addresses

### Retrieve

Populates the Locked MAC Addresses table with a list of the MAC addresses currently locked on the selected device.

### Add

Opens the [Add Static MAC window](#), where you can create a list of locked MAC addresses for this device.

### Remove

Select a Static locked MAC address and click **Remove** to remove the selected entry from the Locked MAC Addresses table.

### Device

Identifies the device selected in the left panel.

### Port IfName

A description of the port on which the MAC address is locked.

### Index

The index value of the port on which the MAC address is locked.

### MAC Address

The MAC address that is locked.

### Locking Cause

Indicates why the MAC address is locked:

- **Authentication** - Locked as the result of authentication
- **First Arrival** - Locked because it was the first MAC address to access the port
- **Static** - MAC address was added to the list administratively

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

For information on related tasks:

- [How to Configure Devices](#)

For information on related windows:

- [MAC Locking Tab \(My Network/All Devices Folder\)](#)
- [MAC Locking Tab \(Devices Group\)](#)
- [Port Properties - MAC Locking Tab](#)
- [MAC Locking Tab \(Port Group\)](#)
- [Port Properties - General Tab](#)

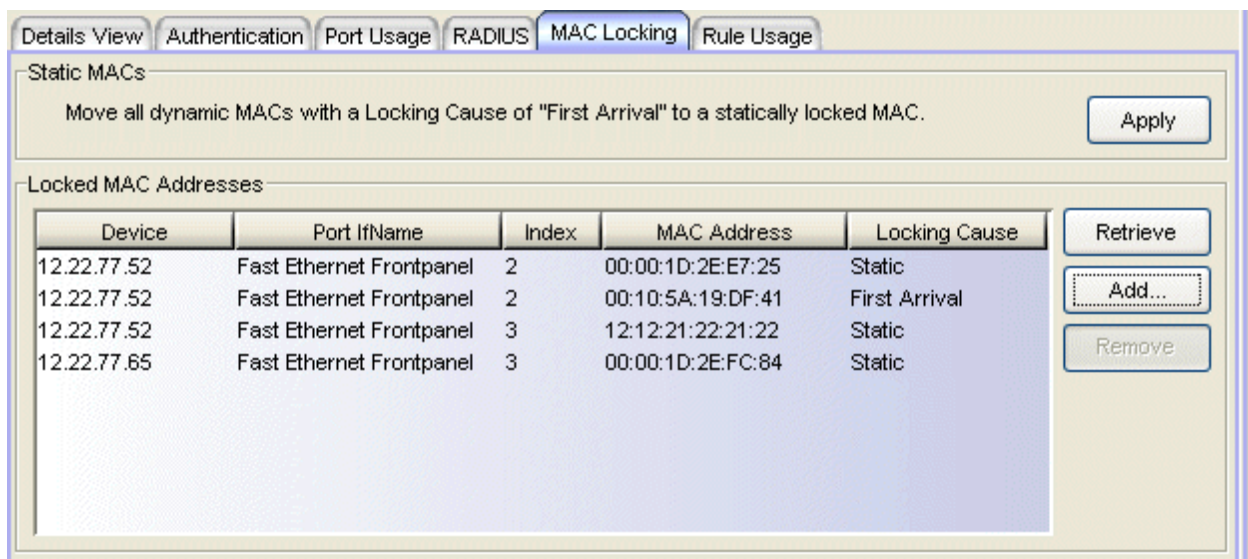
## MAC Locking Tab (Device Group/Island)

This tab displays a list of MAC addresses that are currently locked in a device group, a Policy VLAN Island, or a Network Resource Topology Island, and lets you add and remove addresses on the list. To access this tab:

- select a device group in the left-panel Network Elements tab
- select a VLAN island in the left-panel of the Access Control Configuration window (available from the Policy Manager Edit menu)
- select a topology island in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu)

and click the MAC Locking tab in the right panel. To populate the table, click **Retrieve**.

MAC Locking ensures that only a specific MAC address can access a port, and that traffic from any other MAC addresses will be discarded. See [MAC Locking](#) for more information.



The screenshot shows the MAC Locking configuration window with the following components:

- Navigation tabs: Details View, Authentication, Port Usage, RADIUS, **MAC Locking**, Rule Usage
- Section: Static MACs
- Text: Move all dynamic MACs with a Locking Cause of "First Arrival" to a statically locked MAC.
- Button: Apply
- Section: Locked MAC Addresses
- Table with columns: Device, Port IfName, Index, MAC Address, Locking Cause
- Buttons: Retrieve, Add..., Remove

Device	Port IfName	Index	MAC Address	Locking Cause
12.22.77.52	Fast Ethernet Frontpanel	2	00:00:1D:2E:E7:25	Static
12.22.77.52	Fast Ethernet Frontpanel	2	00:10:5A:19:DF:41	First Arrival
12.22.77.52	Fast Ethernet Frontpanel	3	12:12:21:22:21:22	Static
12.22.77.65	Fast Ethernet Frontpanel	3	00:00:1D:2E:FC:84	Static

### Static MACs

#### Static MACs

Click **Apply** to change all Dynamic Locked MAC addresses (with the [Locking Cause](#) of "First Arrival") to Static Locked MAC addresses. To ensure that all Dynamic Locked MAC addresses are changed to Static,



make sure that the Maximum Number of Static Locked MAC Addresses is set to a large enough value in the [Port Properties MAC Locking Tab](#).

## Locked MAC Addresses

### Retrieve

Populates the Locked MAC Addresses table with a list of the MAC addresses currently locked in the device group or VLAN island.

### Add

Opens the [Add Static MAC window](#), where you can create a list of locked MAC addresses for the device group or VLAN island.

### Remove

Removes the selected entry from the Locked MAC Addresses table.

### Device

Device on which the MAC address is locked.

### Port IfName

A description of the port on which the MAC address is locked.

### Index

The index value of the port on which the MAC address is locked.

### MAC Address

The MAC address that is locked.

### Locking Cause

Indicates why the MAC address is locked:

- **Authentication** - Locked as the result of authentication
- **First Arrival** - Locked because it was the first MAC address to access the port
- **Static** - MAC address was added to the list administratively

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

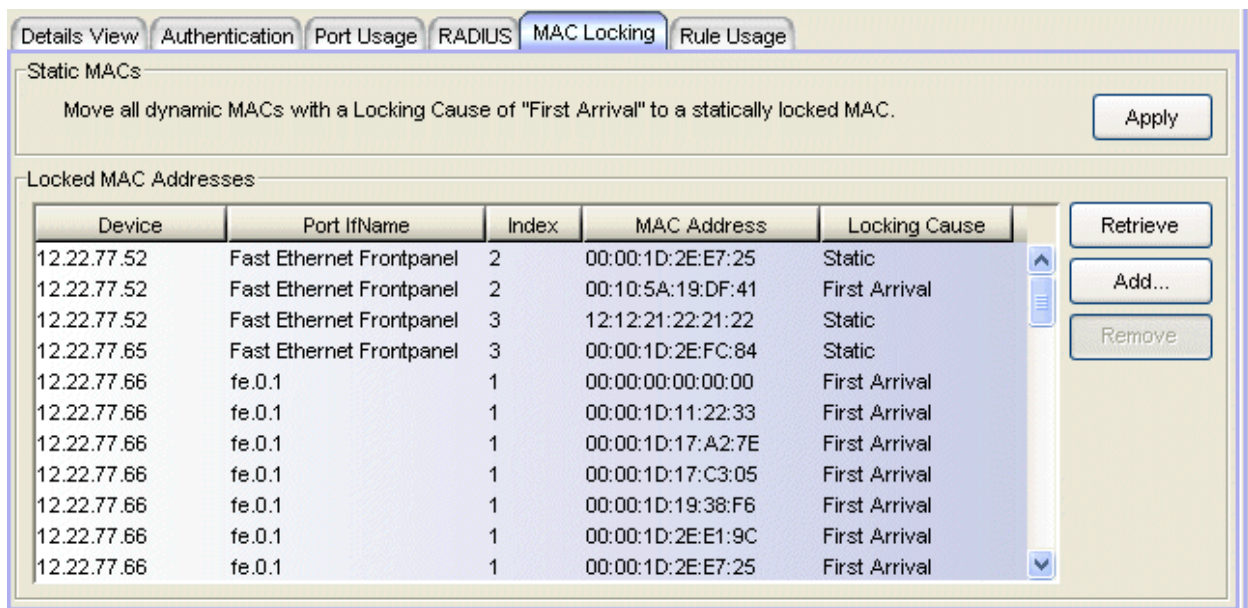
For information on related windows:

- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(My Network/All Devices Folder\)](#)
- [Port Properties - MAC Locking Tab](#)
- [MAC Locking Tab \(Port Group\)](#)
- [Port Properties - General Tab](#)

## MAC Locking Tab (My Network/All Devices Folder)

This MAC Locking tab displays a list of MAC addresses that are currently locked on all the devices in the current domain, and lets you add and remove addresses on the list. To access this tab, select either the My Network or the All Devices folder in the left-panel Network Elements tab, and click the MAC Locking tab in the right panel. You must click **Retrieve** to display the MAC Locking information in the table.

MAC Locking ensures that only a specific MAC address can access a port, and that traffic from any other MAC addresses will be discarded. See [MAC Locking](#) for more information.



Static MACs

Move all dynamic MACs with a Locking Cause of "First Arrival" to a statically locked MAC.

Locked MAC Addresses

Device	Port IfName	Index	MAC Address	Locking Cause
12.22.77.52	Fast Ethernet Frontpanel	2	00:00:1D:2E:E7:25	Static
12.22.77.52	Fast Ethernet Frontpanel	2	00:10:5A:19:DF:41	First Arrival
12.22.77.52	Fast Ethernet Frontpanel	3	12:12:21:22:21:22	Static
12.22.77.65	Fast Ethernet Frontpanel	3	00:00:1D:2E:FC:84	Static
12.22.77.66	fe.0.1	1	00:00:00:00:00:00	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:11:22:33	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:17:A2:7E	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:17:C3:05	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:19:38:F6	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:2E:E1:9C	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:2E:E7:25	First Arrival

### Static MACs

#### Static MACs

Click **Apply** to change all Dynamic Locked MAC addresses (with the [Locking Cause](#) of "First Arrival") to Static Locked MAC addresses. To ensure that all Dynamic Locked MAC addresses are changed to Static, make sure that the Maximum Number of Static Locked MAC Addresses is set to a large enough value in the [Port Properties MAC Locking Tab](#).

## Locked MAC Addresses

### Device

Device on which the MAC address is locked.

### Port IfName

A description of the port on which the MAC address is locked.

### Index

The index value of the port on which the MAC address is locked.

### MAC Address

The MAC address that is locked.

### Locking Cause

Indicates why the MAC address is locked:

- **Authentication** - Locked as the result of authentication
- **First Arrival** - Locked because it was the first MAC address to access the port
- **Static** - MAC address was added to the list administratively

### Retrieve Button

Populates the Locked MAC Addresses table with a list of the MAC addresses currently locked on the devices in the folder.

### Add Button

Opens the [Add Static MAC window](#), where you can create a list of locked MAC addresses for the Devices folder.

### Remove Button

Removes the selected entry from the Locked MAC Addresses table.

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

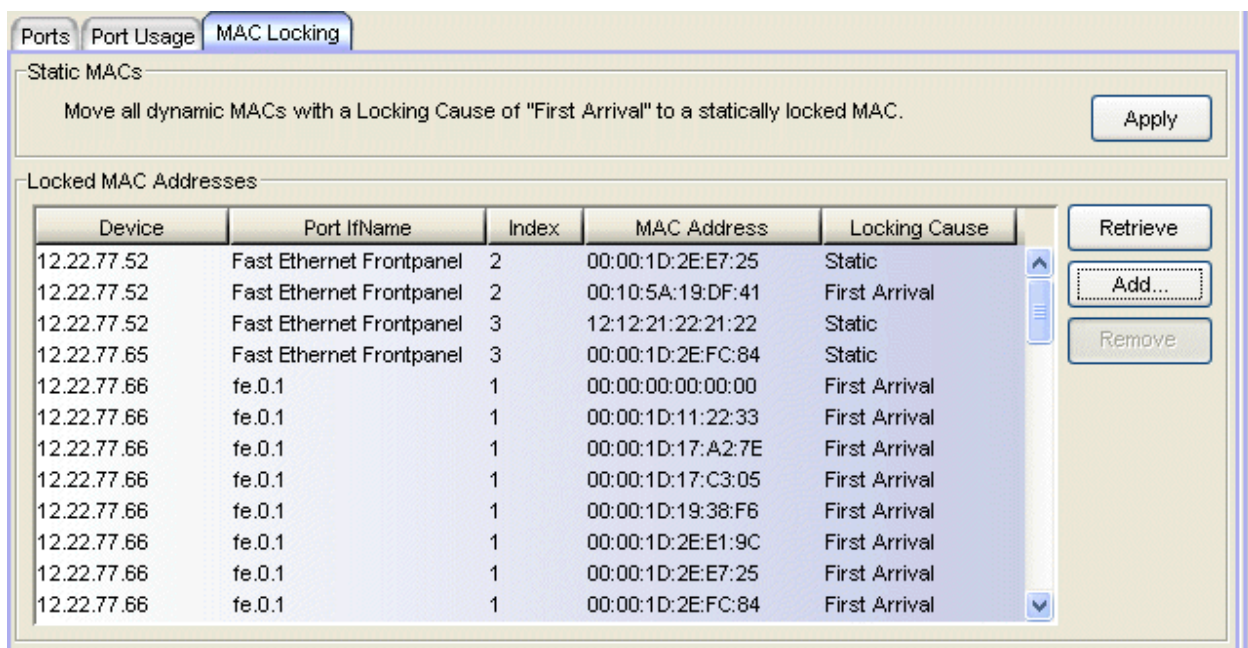
For information on related windows:

- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(Device Group\)](#)

## MAC Locking Tab (Port Group)

This tab displays a list of MAC addresses that are currently locked in a port group, and lets you add and remove addresses on the list. To access this tab, select a port group on the left-panel Port Groups tab and click the MAC Locking tab in the right panel. To populate the table, click **Retrieve**.

MAC Locking ensures that only a specific MAC address can access a port, and that traffic from any other MAC addresses will be discarded. See [MAC Locking](#) for more information



Static MACs

Move all dynamic MACs with a Locking Cause of "First Arrival" to a statically locked MAC. Apply

Locked MAC Addresses

Device	Port IfName	Index	MAC Address	Locking Cause
12.22.77.52	Fast Ethernet Frontpanel	2	00:00:1D:2E:E7:25	Static
12.22.77.52	Fast Ethernet Frontpanel	2	00:10:5A:19:DF:41	First Arrival
12.22.77.52	Fast Ethernet Frontpanel	3	12:12:21:22:21:22	Static
12.22.77.65	Fast Ethernet Frontpanel	3	00:00:1D:2E:FC:84	Static
12.22.77.66	fe.0.1	1	00:00:00:00:00:00	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:11:22:33	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:17:A2:7E	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:17:C3:05	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:19:38:F6	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:2E:E1:9C	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:2E:E7:25	First Arrival
12.22.77.66	fe.0.1	1	00:00:1D:2E:FC:84	First Arrival

Retrieve Add... Remove

## Static MACs

### Static MACs

Click **Apply** to change all Dynamic Locked MAC addresses (with the [Locking Cause](#) of "First Arrival") to Static Locked MAC addresses. To ensure that all Dynamic Locked MAC addresses are changed to Static, make sure that the Maximum Number of Static Locked MAC Addresses is set to a large enough value in the [Port Properties MAC Locking Tab](#).

## Locked MAC Addresses

### Retrieve Button

Populates the Locked MAC Addresses table with a list of the MAC addresses currently locked in the port group.

### Add Button

Opens the [Add Static MAC window](#), where you can create a list of locked MAC addresses for this port group.

### Remove Button

Removes the selected entry from the Locked MAC Addresses table.

### Device

Device on which the MAC address is locked.

### Port IfName

A description of the port on which the MAC address is locked.

### Index

The index value of the port on which the MAC address is locked.

### MAC Address

The MAC address that is locked.

### Locking Cause

Indicates why the MAC address is locked:

- **Authentication** - Locked as the result of authentication
- **First Arrival** - Locked because it was the first MAC address to access the port
- **Static** - MAC address was added to the list administratively

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

For information on related windows:

- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(Device Group\)](#)

- [MAC Locking Tab \(My Network/All Devices Folder\)](#)
- [Port Properties - MAC Locking Tab](#)

## Mappings Tab (Role)

This tab lets you view and configure four different mapping lists for the selected role:

- **MAC to Role Mapping** - Lets you assign the role to an end user based on the user's MAC address.
- **IP to Role Mapping** - Lets you assign the role to an end user based on the user's IP address.
- **Tagged Packet VLAN to Role Mapping** - Lets you assign the role to network traffic based on the traffic's VLAN ID.
- **Authentication-Based VLAN to Role Mapping** - Lets you assign the role to an end user during the authentication process, based on a VLAN Attribute.

To access this tab, select a role in the left panel's Roles tab and click the Mappings tab in the right panel. Any additions or changes you make to this tab must be [enforced](#) in order to take effect.

The screenshot shows the 'Mappings' tab for a role configuration. It features four distinct mapping sections, each with a table and control buttons.

**MAC to Role Mapping**

Device/Port Level	MAC Address	Source/Destination
Device Level	00:00:1d:88:88:48	Source
[10.20.77.33] Port fe.1.10	00:01:1f:df:21:bd48	Destination

**IP to Role Mapping**

IP	Source/Destination
10.20.30.40/32	Source
10.20.30.50/32	Destination

**Tagged Packet VLAN to Role Mapping**

NOTE: To forward traffic w/ VLAN & CoS specified by this Role, TCI Overwrite must be enabled. C2/B2/D2/C3/B3/G3/C5/B5/A4 devices support rewriting CoS value but not the VLAN.  
\* - Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping.

* Device/Port Level	CoS
Device Level	54
Device Level	5

**Authentication Based VLAN to Role Mapping**

VLAN
4[VLAN 4]




## MAC to Role Mapping

MAC to Role mapping provides a way to assign a role to an end station based on its MAC address. This allows you to create a specific role for a group of end stations (such as IP phones), and assign it to them based on their MAC address. When the end stations connect to the network, the policy-enabled device identifies the source MAC address and applies the mapped role.

This table lists any device-level (all devices) or port-level MAC to Role mappings that have been configured for this role. Use the **Add** button to create a new device-level mapping for this role. Port-level mappings can be added via the [Port Properties General tab, Mappings Sub-tab](#). Port-level mappings will override any device-level mappings.

**NOTES:** -- You must have the Port Level Role Mappings feature enabled in Policy Manager for port-level mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored and any mappings listed here will be grayed out.

-- Port-level mappings cannot be added to or removed from frozen ports . You must clear the frozen state on a port in order to add or remove a mapping. Once you have created a mapping, you can freeze the port. The port-level mappings of the frozen port will still be enforced and verified.

### Device/Port Level

This column indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description).

### MAC Address

The MAC addresses mapped to this role. Click **Add** to add a MAC address and mask to the list. Using a mask provides an easy way to select end stations based on a portion of their MAC address. For example, you could select one MAC address, then use a mask based on the manufacturers ID portion of the MAC address to specify all your Siemens IP Phones. Masked MAC addresses are not supported on legacy devices.

### Source/Destination

Specifies whether the MAC address is a source or destination address.

### Add

Opens the Add MAC Address window, where you can select a MAC address and specify the direction (source or destination).

### Remove

Select a MAC address and click **Remove** to remove the mapping from the list.

## IP to Role Mapping

IP to Role mapping provides a way to assign a role to an end station based on its IP address. For example, in networks that haven't deployed authentication, this would allow you to map an individual IP address such as an administrator's laptop, to a specific role. When the end station connects to the network, the policy-enabled device identifies the IP address and applies the mapped role.

This table lists any IP to Role mappings that have been configured for this role. Use the **Add** button to create a new mapping for this role.

### IP Address

The IP addresses mapped to this role. Click **Add** to add an IP address (IPv4 or IPv6 address) and mask to the list. Masked IP addresses are not supported on legacy devices.

### Source/Destination

Specifies whether the IP address is a source or destination address.

### Add

Opens the Add IP Address window, where you can enter an IP address (IPv4 or IPv6 address) and specify the direction (source or destination).

### Remove

Select an IP address and click **Remove** to remove the mapping from the list.


## Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. For more information, see [VLAN to Role Mapping](#) in the Concepts Help topic.

This table lists any device-level (all devices) or port-level Tagged Packet VLAN to Role mappings that have been configured for this role. Use the **Add** button to create a new device-level mapping for this role. Port-level mappings can be

added via the [Port Properties General tab, Mappings Sub-tab](#). Port-level mappings will override any device-level mappings.

**NOTES:** -- You must have the Port Level Role Mappings feature enabled in Policy Manager for port-level mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored and any mappings listed here will be grayed out.

-- Port-level mappings cannot be added to or removed from frozen ports . You must clear the frozen state on a port in order to add or remove a mapping. Once you have created a mapping, you can freeze the port. The port-level mappings of the frozen port will still be enforced and verified.

**NOTE: TCI Overwrite Requirement**

-- Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a COS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.

-- If supported by the device, you can enable TCI Overwrite on a per-port basis in the [Port Properties window General tab](#), or for an individual role in the role's [General tab](#). The stackable devices support rewriting the CoS values but not the VLAN ID.

**\* - Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping**

Use this column to select the device-level VLAN to role mapping that will be used for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make a selection, there will be no device-level mapping for these devices. Use the Mappings tab in the [Enforce Preview window](#) to quickly see which VLAN to role mapping is selected for these devices.

**Device/Port Level**

This column indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description).

**VLAN**

The VLAN ID and name of the VLANs mapped to this role. Click **Add** to add a VLAN to the list.

**Add**

Opens the VLANs [Selection View](#), where you can choose a VLAN to map to the role.

**Remove**

Select a VLAN and click **Remove** to remove the mapping from the list.

## Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Use this table to view and configure the VLANs that will map to the selected role. For more information, see [VLAN to Role Mapping](#) in the Concepts Help topic.

This table lists any Authentication-Based VLAN to Role mappings that have been configured for this role. Use the **Add** button to create a new mapping for this role.

---

**NOTE:** When configuring Authentication-Based VLAN to role mapping, you must enable RFC3580 VLAN Authorization on the device via the [device Authentication tab](#).

---

**VLAN**

The VLAN ID and name of the VLANs mapped to this role. Click **Add** to add a VLAN to the list.

**Add**

Opens the VLANs [Selection View](#), where you can choose a VLAN to map to the role.

**Remove**

Select a VLAN and click **Remove** to remove the VLAN from the list.

---

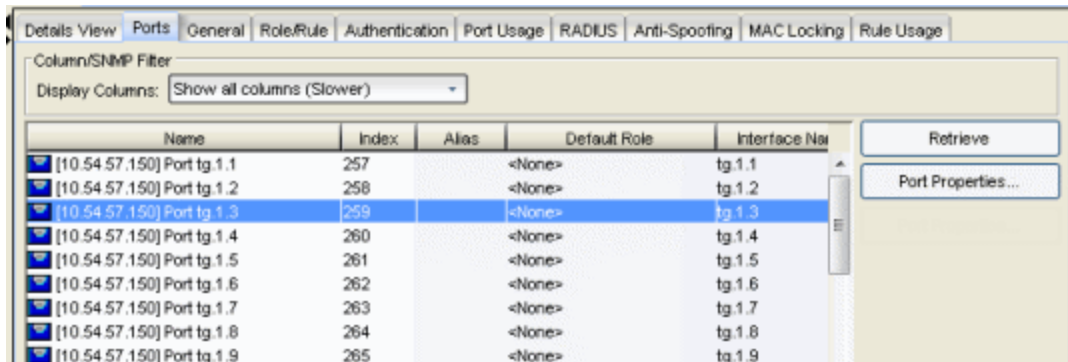
### Related Information

For information on related concepts:

- [VLAN to Role Mapping](#)

## Ports Tab (Device)

The device Ports tab displays a table of information about the selected device's ports. To access this tab, select a device on the left panel's Network Elements tab and click the Ports tab in the right panel. Right-click an item in the table to see a menu of available options.



The screenshot shows the 'Ports' tab in a network management interface. At the top, there are several tabs: 'Details View', 'Ports', 'General', 'Role/Rule', 'Authentication', 'Port Usage', 'RADIUS', 'Anti-Spoofing', 'MAC Locking', and 'Rule Usage'. Below the tabs is a 'Column/SNMP Filter' section with a dropdown menu set to 'Show all columns (Slower)'. The main area contains a table with the following columns: 'Name', 'Index', 'Alias', 'Default Role', and 'Interface Name'. The table lists ports from tg.1.1 to tg.1.9. The 'Port tg.1.3' row is highlighted in blue. To the right of the table are two buttons: 'Retrieve' and 'Port Properties...'. The table data is as follows:

Name	Index	Alias	Default Role	Interface Name
[10.54.57.150] Port tg.1.1	257		<None>	tg.1.1
[10.54.57.150] Port tg.1.2	258		<None>	tg.1.2
[10.54.57.150] Port tg.1.3	259		<None>	tg.1.3
[10.54.57.150] Port tg.1.4	260		<None>	tg.1.4
[10.54.57.150] Port tg.1.5	261		<None>	tg.1.5
[10.54.57.150] Port tg.1.6	262		<None>	tg.1.6
[10.54.57.150] Port tg.1.7	263		<None>	tg.1.7
[10.54.57.150] Port tg.1.8	264		<None>	tg.1.8
[10.54.57.150] Port tg.1.9	265		<None>	tg.1.9

### Column/SNMP Filter

Port data retrieval requires many SNMP queries and can cause significant wait times to fill in the requested port details view. High network latency environments are most impacted by the delay. Use this menu to hide unnecessary columns to improve performance by reducing SNMP overhead.

- **Show all columns (Slower)** - Lets you view all port details.
- **Show only basic columns (Fastest)** - Hides some columns of information to lower SNMP overhead and allow faster retrieval times of port data.
- **Show optional columns (Faster)** - Display one or more of the hidden columns by selecting an optional column checkbox.

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Alias

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

### Default Role

Displays the default role for the port. To set the default role, select a port, right-click and select Set Default Role. The Roles Selection view appears where you can select the desired default role. See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

---

**NOTE:** Setting a default role on an ExtremeWireless Wireless Controller port that is not yet a VNS, creates a new VNS on the HWC.

---

### Interface Name

A description of the port.

### Egress Policy

Displays whether [egress policy](#) is enabled, disabled, or not supported (N/A) for the port.

### Port Type

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

### Port Speed

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

### Port Mode

[Port mode](#) as set in the [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

### Device Auth Mode

Authentication type(s) configured on the device ([Quarantine](#), [802.1X](#), [Web-Based](#), [MAC](#), [CEP](#), [Auto Tracking](#), or None). Some devices support multiple authentication types and multiple users (Multi-User authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User authentication). If the value is None, all types of authentication are disabled at the device level, and port authentication settings cannot be configured and will not take effect.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

**TCI Overwrite**

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

**MAC Locking**

Indicates whether or not [MAC locking](#) is enabled on the port.

**Retrieve Button**

Retrieves the most recent information about the ports on the device.

**Port Properties Button**

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

**Related Information**

For information on related tasks:

- [Authentication Configuration Guide](#)
- [802.1X Authentication Configuration Supplement](#)
- [How to Create a Port Group](#)
- [Using the Port Configuration Wizard](#)
- [Using the Device Configuration Wizard](#)

For information on related windows:

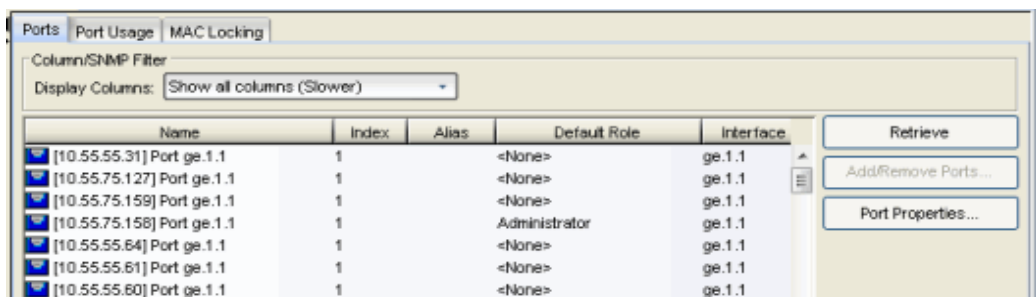
- [Port Properties - Authentication Configuration Tab](#)
- [RADIUS Tab \(Device\)](#)

## Ports Tab (Port Group)

The port group Ports tab provides a table of information about the ports in the selected port group. It also includes buttons that enable you to retrieve the latest information about the ports, access the Port Properties windows, and add and remove ports (user-defined port groups only). To access this tab, select a port group in the left-panel Port Groups tab, then select the Ports tab in the right panel.

If you have selected a User-Defined Port group, you will also see a General section that contains the name and description of the port group, with an **Edit** button to change the description, if desired.

See [Pre-Defined Port Groups](#) for more information on the port groups provided by Policy Manager.



The screenshot shows a software interface with a 'Ports' tab selected. At the top, there are tabs for 'Ports', 'Port Usage', and 'MAC Locking'. Below the tabs is a 'Column/SNMP Filter' section with a dropdown menu set to 'Show all columns (Slower)'. The main area contains a table with the following columns: Name, Index, Alias, Default Role, and Interface. The table lists six ports, all with an index of 1 and interface of ge.1.1. The 'Alias' column contains '<None>' for five ports and 'Administrator' for one. To the right of the table are three buttons: 'Retrieve', 'Add/Remove Ports...', and 'Port Properties...'.

Name	Index	Alias	Default Role	Interface
[10.55.55.31] Port ge.1.1	1	<None>	<None>	ge.1.1
[10.55.75.127] Port ge.1.1	1	<None>	<None>	ge.1.1
[10.55.75.159] Port ge.1.1	1	<None>	<None>	ge.1.1
[10.55.75.158] Port ge.1.1	1	Administrator	<None>	ge.1.1
[10.55.55.64] Port ge.1.1	1	<None>	<None>	ge.1.1
[10.55.55.61] Port ge.1.1	1	<None>	<None>	ge.1.1
[10.55.55.60] Port ge.1.1	1	<None>	<None>	ge.1.1

### Column/SNMP Filter

Port data retrieval requires many SNMP queries and can cause significant wait times to fill in the requested port details view. High network latency environments are most impacted by the delay. Use this menu to hide unnecessary columns to improve performance by reducing SNMP overhead.

- **Show all columns (Slower)** - Lets you view all port details.
- **Show only basic columns (Fastest)** - Hides some columns of information to lower SNMP overhead and allow faster retrieval times of port data.
- **Show optional columns (Faster)** - Display one or more of the hidden columns by selecting an optional column checkbox.

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.



**Index**

The index value assigned to the port interface.

**Alias**

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

**Default Role**

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

**Interface Name**

The port interface name.

**Egress Policy**

Displays whether [egress policy](#) is enabled, disabled, or not supported (N/A) for the port.

**Port Type**

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

**Port Speed**

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

**Port Mode**

[Port mode](#) as set in the port's [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

**Device Authentication Type(s)**

Authentication type(s) configured on the device ([802.1X](#), [Web-Based](#), [MAC](#), [CEP](#) or None). Some devices support multiple authentication types and multiple users (Multi-User authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User authentication). If the value is None, all types of authentication are disabled at the device level, and port authentication settings cannot be configured and will not take effect.

**Drop VLAN Tagged Frames**

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

**TCI Overwrite**

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not

Applicable) for this column.

**MAC Locking**

Indicates whether or not [MAC locking](#) is enabled on the port.

**Retrieve Button**

Retrieves the most recent information about the ports in the port group.

**Add/Remove Ports Button**

Selecting a port in the table and clicking this button opens the [Add/Remove Ports window](#), which enables you to add and remove ports to and from the port group. This option is available for user-defined port groups only.

**Port Properties Button**

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

**Related Information**

For information on related tasks:

- [How to Configure Ports](#)

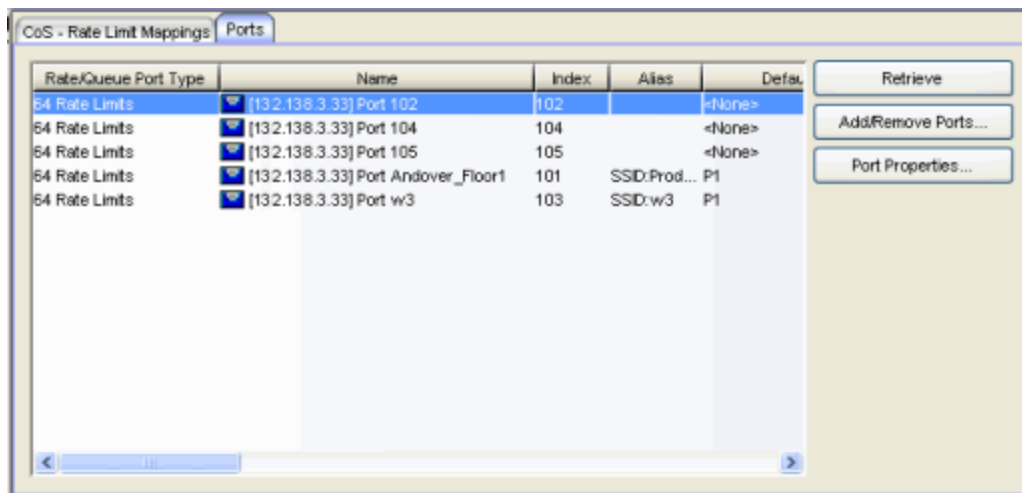
For information on related windows:

- [Add/Remove Ports Window](#)
- [Port Properties - Authentication Configuration Tab](#)
- [Port Properties - Port Usage Tab](#)
- [Port Properties - General Tab](#)

## Ports Tab (Rate Limit Port Group)

The rate limit port group Ports tab lets you view all the ports in the selected port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information (via the port's General tab). Click the **Retrieve** button to retrieve the latest port information for the group.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a rate limit port group in the tree, and then select the Ports tab in the right panel.



### Rate/Queue Port Type

The number of rate limits the port supports.

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Alias

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

**Default Role**

The default role assigned to the port. See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

**Current Role**

Current role assigned to the port, through successful authentication or assignment of the default role. This is determined by the device, based on the configuration settings that have been applied to the port ([Port Properties Authentication Configuration tab](#)).

**Interface Name**

A description of the port.

**Port Type**

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

**Port Speed**

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

**User Name**

User ID of the user currently or most recently authenticated on the port.

**Port Mode**

[Port mode](#) as set in the port's [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

**Authentication State**

Current state of the port with regard to authentication. If "None," authentication is not enabled on the device. Devices that support multiple authenticated users per port will display N/A (Not Applicable) for this column.

For web-based authentication:

- **Disconnected** - There is no end user currently logged in on the port.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.

- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.

For 802.1X authentication:

- **Initialize** - The port is initializing. One reason for this is that the device has been reset.
- **Disconnected** - There is no end user currently logged in on the port.
- **Connecting** - The port is establishing communication with an end user.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Aborting** - The authentication procedure is being prematurely terminated due to, for example, a re-authentication request or an authentication timeout.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.
- **Default Role** - An end user has connected and is using the port's default role. Occurs when the port mode is set to Inactive/Default (see [Port Mode](#) for more information).
- **No Authentication** - No end user can be authenticated because the port mode is set to Inactive/Discard (see [Port Mode](#) for more information).

### Last Login Result

(Web-based authentication only) Indicates the result (success/failure) of the last attempt to log in to this port. Possible results are as follows:

- **Not logged in since last reset** - No login in since reset.
- **Authentication accepted** - User logged in successfully.
- **Authentication rejected**
  - Username or password mismatch
  - User misconfiguration (e.g. Deny Remote Permission in Active Directory Users).

- or, when two RADIUS servers are configured in the device:
  - Mismatched Shared Secret in a primary RADIUS server or both RADIUS servers.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown policy** - No policy (Role) defined in the device.
- **Unknown authentication server response** - When one RADIUS server is configured in the device:
  - Wrong Authentication UDP port number defined.
  - Mismatched Shared Secret.
  - RADIUS server is not contactable, or RADIUS server is down.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown authentication client error** - User enters no username and password.
- **Auth client disabled or unavailable** - RADIUS server is disabled in the device.
- **Port authentication pending** - Port is in the process of authenticating.
- **Port held for too many failed attempts** - User reached the maximum number of failed attempts to log in.
- **Port held: Max attempts exceeded** - User exceeded the maximum number of failed attempts to log in once the port has been held.
- **Authentication server timeout** - When two RADIUS servers are configured in the device:
  - Wrong Authentication UDP port number defined in a primary RADIUS server or both RADIUS servers.
  - RADIUS servers are not contactable
  - Unsupported protocol (e.g. CHAP) configured on the device.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

### TCI Overwrite

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

### MAC Locking

Indicates whether or not [MAC locking](#) is enabled on the port.

### Retrieve Button

Retrieves the most recent information about the ports in the rate limit port group.

### Add/Remove Ports Button

Opens the [Add/Remove Ports window](#), where you can add and remove ports to and from the port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

### Port Properties Button

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Define Rate Limits](#)
- [Creating Class of Service Port Groups](#)

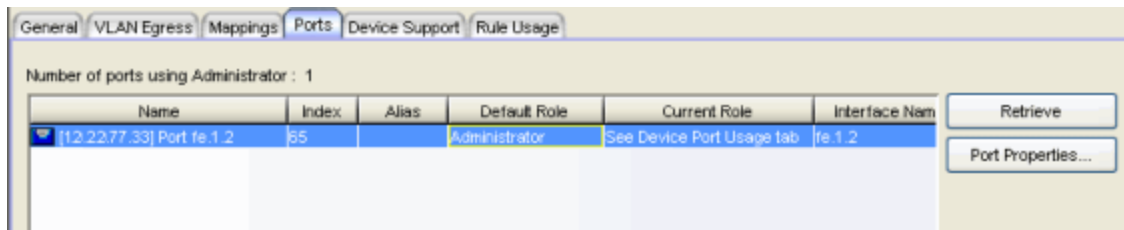
For information on related windows:

- [CoS - Rate Limits Mappings Tab \(Rate Limit Port Group\)](#)

## Ports Tab (Role)

---

The Ports tab lists the ports currently authenticated to the selected role, and/or having the role set as its [default role](#). It includes buttons that enable you to retrieve the latest information about the ports, and view and edit port information (via the Roles tab for the port). To access this tab, select a role in the left panel's Roles tab, then select the Ports tab in the right panel.



Name	Index	Alias	Default Role	Current Role	Interface Name
[12.22.77.33] Port fe.1.2	65		Administrator	See Device Port Usage tab	fe.1.2

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Alias

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

### Default Role

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

### Current Role

Current role assigned to the port, through successful authentication or assignment of the default role. This is determined by the device, based on the configuration settings that have been applied to the port (Authentication Settings). See [Port Mode](#) for more information.

### Interface Name

A description of the port.

### Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.



### Port Speed

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

### User Name

User ID provided by the authenticated end user.

### Port Mode

[Port mode](#) as set in the port's [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

### Authentication State

Current state of the port with regard to authentication. If "None", authentication is not enabled on the device. Devices that support multiple authenticated users per port will display N/A (Not Applicable) for this column.

For web-based authentication:

- **Disconnected** - There is no end user currently logged in on the port.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.

For 802.1X authentication:

- **Initialize** - The port is initializing. One reason for this is that the device has been reset.
- **Disconnected** - There is no end user currently logged in on the port.
- **Connecting** - The port is establishing communication with an end user.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Aborting** - The authentication procedure is being prematurely terminated due to, for example, a re-authentication request or an authentication timeout.

- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.
- **Default Role** - An end user has connected and is using the port's default role. Occurs when the port mode is set to Inactive/Default (see [Port Mode](#) for more information).
- **No Authentication** - No end user can be authenticated because the port mode is set to Inactive/Discard (see [Port Mode](#) for more information).

### Last Login Result

(Web-based authentication only) Indicates the result (success/failure) of the last attempt to log in to this port. Possible results are as follows:

- **Not logged in since last reset** - No login in since reset.
- **Authentication accepted** - User logged in successfully.
- **Authentication rejected**
  - Username or password mismatch
  - User misconfiguration (e.g. Deny Remote Permission in Active Directory Users).or, when two RADIUS servers are configured in the device:
  - Mismatched Shared Secret in a primary RADIUS server or both RADIUS servers.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown policy** - No policy (Role) defined in the device.
- **Unknown authentication server response** - When one RADIUS server is configured in the device:
  - Wrong Authentication UDP port number defined.
  - Mismatched Shared Secret.
  - RADIUS server is not contactable, or RADIUS server is down.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown authentication client error** - User enters no username and password.
- **Auth client disabled or unavailable** - RADIUS server is disabled in the device.
- **Port authentication pending** - Port is in the process of authenticating.

- **Port held for too many failed attempts** - User reached the maximum number of failed attempts to log in.
- **Port held: Max attempts exceeded** - User exceeded the maximum number of failed attempts to log in once the port has been held.
- **Authentication server timeout** - When two RADIUS servers are configured in the device:
  - Wrong Authentication UDP port number defined in a primary RADIUS server or both RADIUS servers.
  - RADIUS servers are not contactable
  - Unsupported protocol (e.g. CHAP) configured on the device.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

### TCI Overwrite

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

### MAC Locking

Indicates whether or not [MAC locking](#) is enabled on the port.

### Retrieve Button

Retrieves/updates the list of ports associated with this role.

### Port Properties Button

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

## Related Information

For information on related concepts:

- [Authentication](#)
- [Role](#)

For information on related tasks:

- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

- [Using the Device Configuration Wizard](#)
- [Using the Port Configuration Wizard](#)

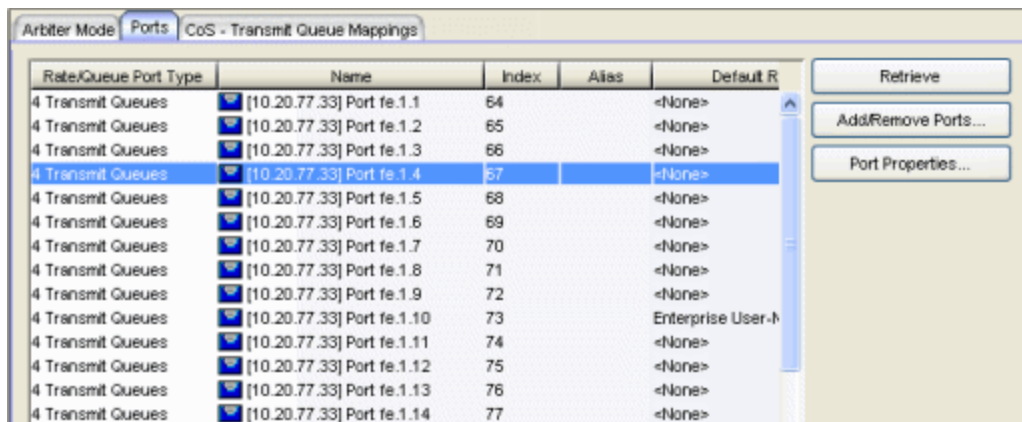
For information on related windows:

- [Port Properties - Authentication Configuration Tab](#)
- [RADIUS Tab \(Device\)](#)
- [Port Properties - General Tab](#)

## Ports Tab (Transmit Queue Port Group)

The Ports tab lets you view all the ports in the selected transmit queue port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information (via the port's General tab). Click the **Retrieve** button to retrieve the latest port information for the group.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a transmit queue port group in the tree, and then select the Ports tab in the right panel.



Rate/Queue Port Type	Name	Index	Alias	Default R
4 Transmit Queues	[10.20.77.33] Port fe.1.1	64		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.2	65		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.3	66		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.4	67		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.5	68		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.6	69		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.7	70		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.8	71		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.9	72		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.10	73		Enterprise User-1
4 Transmit Queues	[10.20.77.33] Port fe.1.11	74		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.12	75		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.13	76		<None>
4 Transmit Queues	[10.20.77.33] Port fe.1.14	77		<None>

### Rate/Queue Port Type

The number of transmit queues the port supports.

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Alias

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

### Default Role

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

### Current Role

Current role assigned to the port, through successful authentication or assignment of the default role. This is determined by the device, based on the configuration settings that have been applied to the port ([Port Properties Authentication Configuration tab](#)).

### Interface Name

A description of the port.

### Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

### Port Speed

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

### User Name

User ID of the user currently or most recently authenticated on the port.

### Port Mode

[Port mode](#) as set in the port's [Port Properties Authentication Configuration tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

### Authentication State

Current state of the port with regard to authentication. If "None," authentication is not enabled on the device. Devices that support multiple authenticated users per port will display N/A (Not Applicable) for this column.

For web-based authentication:

- **Disconnected** - There is no end user currently logged in on the port.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.

For 802.1X authentication:

- **Initialize** - The port is initializing. One reason for this is that the device has been reset.
- **Disconnected** - There is no end user currently logged in on the port.
- **Connecting** - The port is establishing communication with an end user.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Aborting** - The authentication procedure is being prematurely terminated due to, for example, a re-authentication request or an authentication timeout.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.
- **Default Role** - An end user has connected and is using the port's default role. Occurs when the port mode is set to Inactive/Default (see [Port Mode](#) for more information).
- **No Authentication** - No end user can be authenticated because the port mode is set to Inactive/Discard (see [Port Mode](#) for more information).

### Last Login Result

(Web-based authentication only) Indicates the result (success/failure) of the last attempt to log in to this port. Possible results are as follows:

- **Not logged in since last reset** - No login in since reset.
- **Authentication accepted** - User logged in successfully.
- **Authentication rejected**
  - Username or password mismatch
  - User misconfiguration (e.g. Deny Remote Permission in Active Directory Users).

or, when two RADIUS servers are configured in the device:

- Mismatched Shared Secret in a primary RADIUS server or both RADIUS servers.
- Unsupported protocol (e.g. CHAP) configured on the device.

- **Unknown policy** - No policy (Role) defined in the device.
- **Unknown authentication server response** - When one RADIUS server is configured in the device:
  - Wrong Authentication UDP port number defined.
  - Mismatched Shared Secret.
  - RADIUS server is not contactable, or RADIUS server is down.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown authentication client error** - User enters no username and password.
- **Auth client disabled or unavailable** - RADIUS server is disabled in the device.
- **Port authentication pending** - Port is in the process of authenticating.
- **Port held for too many failed attempts** - User reached the maximum number of failed attempts to log in.
- **Port held: Max attempts exceeded** - User exceeded the maximum number of failed attempts to log in once the port has been held.
- **Authentication server timeout** - When two RADIUS servers are configured in the device:
  - Wrong Authentication UDP port number defined in a primary RADIUS server or both RADIUS servers.
  - RADIUS servers are not contactable
  - Unsupported protocol (e.g. CHAP) configured on the device.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

### TCI Overwrite

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

### MAC Locking

Indicates whether or not [MAC locking](#) is enabled on the port.

### Retrieve Button

Retrieves the most recent information about the ports in the transmit queue port group.



### Add/Remove Ports Button

Opens the [Add/Remove Ports window](#), where you can add and remove ports to and from the port group.

### Port Properties Button

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

For information on related windows:

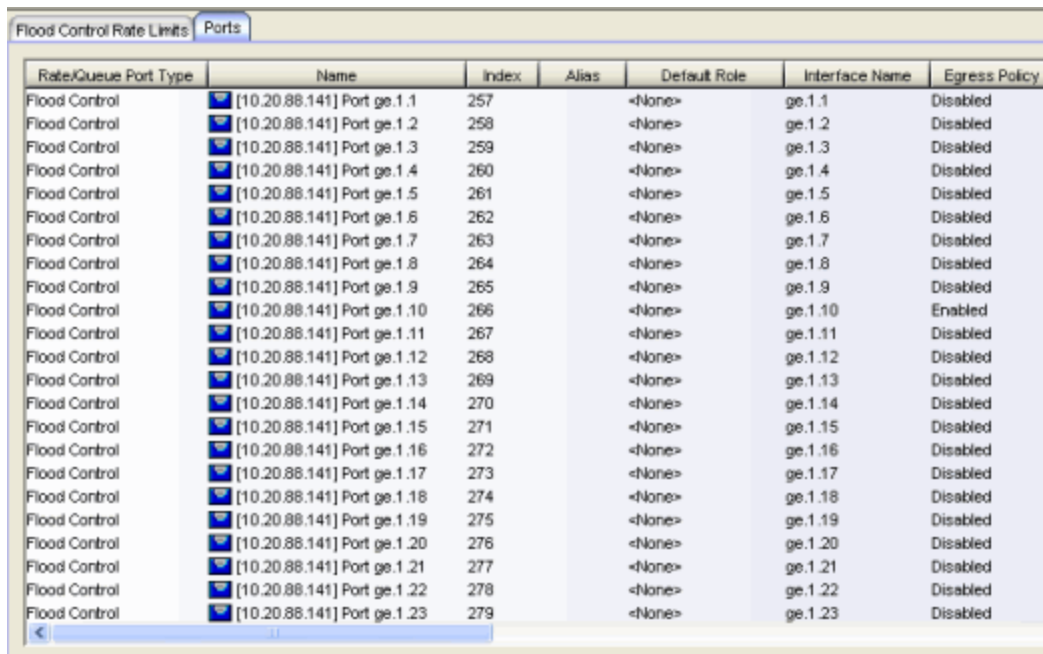
- [Arbiter Mode Tab \(Transmit Queue Port Group\)](#)
- [CoS - Transmit Queue Mappings Tab \(Transmit Queue Port Group\)](#)

## Ports Tab (Flood Control Port Groups)

The flood control port group Ports tab provides a table of information about the ports in the selected port group. It also includes buttons that enable you to retrieve the latest information about the ports and to add and remove ports. To access this tab, select a port group in the left-panel Flood Control Port Groups, then select the Ports tab in the right panel.

**NOTES:** The Ports Tab is only available when a Flood Control port group is selected, and when advanced mode is enabled on the [CoS Configuration Window](#).

The actual columns that appear under the Ports tab might vary based on the Port Details View and SNMP options settings on the [Policy Manager Options Window](#).



Rate/Queue Port Type	Name	Index	Alias	Default Role	Interface Name	Egress Policy
Flood Control	[10.20.88.141] Port ge.1.1	257		<None>	ge.1.1	Disabled
Flood Control	[10.20.88.141] Port ge.1.2	258		<None>	ge.1.2	Disabled
Flood Control	[10.20.88.141] Port ge.1.3	259		<None>	ge.1.3	Disabled
Flood Control	[10.20.88.141] Port ge.1.4	260		<None>	ge.1.4	Disabled
Flood Control	[10.20.88.141] Port ge.1.5	261		<None>	ge.1.5	Disabled
Flood Control	[10.20.88.141] Port ge.1.6	262		<None>	ge.1.6	Disabled
Flood Control	[10.20.88.141] Port ge.1.7	263		<None>	ge.1.7	Disabled
Flood Control	[10.20.88.141] Port ge.1.8	264		<None>	ge.1.8	Disabled
Flood Control	[10.20.88.141] Port ge.1.9	265		<None>	ge.1.9	Disabled
Flood Control	[10.20.88.141] Port ge.1.10	266		<None>	ge.1.10	Enabled
Flood Control	[10.20.88.141] Port ge.1.11	267		<None>	ge.1.11	Disabled
Flood Control	[10.20.88.141] Port ge.1.12	268		<None>	ge.1.12	Disabled
Flood Control	[10.20.88.141] Port ge.1.13	269		<None>	ge.1.13	Disabled
Flood Control	[10.20.88.141] Port ge.1.14	270		<None>	ge.1.14	Disabled
Flood Control	[10.20.88.141] Port ge.1.15	271		<None>	ge.1.15	Disabled
Flood Control	[10.20.88.141] Port ge.1.16	272		<None>	ge.1.16	Disabled
Flood Control	[10.20.88.141] Port ge.1.17	273		<None>	ge.1.17	Disabled
Flood Control	[10.20.88.141] Port ge.1.18	274		<None>	ge.1.18	Disabled
Flood Control	[10.20.88.141] Port ge.1.19	275		<None>	ge.1.19	Disabled
Flood Control	[10.20.88.141] Port ge.1.20	276		<None>	ge.1.20	Disabled
Flood Control	[10.20.88.141] Port ge.1.21	277		<None>	ge.1.21	Disabled
Flood Control	[10.20.88.141] Port ge.1.22	278		<None>	ge.1.22	Disabled
Flood Control	[10.20.88.141] Port ge.1.23	279		<None>	ge.1.23	Disabled

### Rate/Queue Port Type

Shows the selected port type rate/queue.

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Alias

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

### Default Role

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

### Current Role

See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

### Interface Name

The port interface name.

### Egress Policy

Displays whether [egress policy](#) is enabled, disabled, or not supported (N/A) for the port.

### Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

### Port Speed

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

### Port Mode

[Port mode](#) as set in the port's [Port Properties Authentication Configuration](#) [tab](#). If Policy Manager is unable to determine the port mode (e.g., for logical ports), Unknown is displayed.

### Device Authentication Type(s)

Authentication type(s) configured on the device ([802.1X](#), [Web-Based](#), [MAC](#), [CEP](#) or None). Some devices support multiple authentication types and multiple users (Multi-User authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User authentication). If the value is None, all types of authentication are disabled at the device level, and port authentication settings cannot be configured and will not take effect.

### Drop VLAN Tagged Frames

Indicates whether or not the [Drop VLAN Tagged Frames](#) feature is enabled on the port.

### TCI Overwrite

Indicates whether or not [TCI Overwrite](#) is enabled on the port. Ports on devices that do not support TCI Overwrite will display N/A (Not Applicable) for this column.

### MAC Locking

Indicates whether or not [MAC locking](#) is enabled on the port.

### Retrieve Button

Retrieves the most recent information about the ports in the port group.

### Add/Remove Ports Button

Selecting a port in the table and clicking this button opens the [Add/Remove Ports window](#), which enables you to add and remove ports to and from the port group. This option is available for user-defined port groups only.

### Port Properties Button

Select a port in the table and click this button to access the [Port Properties General tab](#) where you can view and edit port information.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Configure Flood Control](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)

## Port Usage Tab (Device)

---

The device Port Usage tab displays information related to end user login ([authentication](#)) sessions, rate limit violations, and CEP (Convergence End Point) connections on a device. To display this tab, select a device in the left-panel Network Elements tab, then click the Port Usage tab in the right panel. You must click **Retrieve** to display the port information in the tables.

The Port Usage tab provides three sub-tabs to allow you to view the desired information:

- [End User Sessions Tab](#)
- [Rate Limit Violations Tab](#)
- [CEP Usage Tab](#)

### End User Sessions Tab

This tab displays information about each login session for the ports on the device, including the current values being collected for a session still in progress, or the final values for the last valid session when there is no session currently active. You must click **Retrieve** to display the port information in the table.

By default the **Show Only Active Sessions** checkbox is checked, and only your active sessions are displayed. Deselect the checkbox to display all entries. Active sessions that are being applied to traffic are listed in blue text. Active sessions that are not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type will be applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC,) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that

do not support multi-authentication, by definition the active session is also applied.

**NOTE:** Devices configured for multi-user authentication always list *only* active sessions even if the Show Only Active Session checkbox is deselected.

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports will be listed in the table, along with the roles under which they are authenticated.

Device	Interface Name	Index	Alias	Type	MAC Address
12.2288.8	ge.1.9	265		MAC	00:1F:45:47:4B:F4
12.2288.8	ge.1.9	265		MAC	00:1F:45:47:4B:F5
12.2288.8	ge.1.10	266		MAC	00:01:F4:40:CB:0E
12.2288.8	ge.1.10	266		MAC	00:11:88:BD:CC:36
12.2288.8	ge.1.11	267		MAC	00:11:88:FD:91:40
12.2288.8	ge.1.12	268		MAC	00:11:88:A9:19:A0
12.2288.8	ge.1.13	269		MAC	00:1F:45:47:76:34
12.2288.8	ge.1.13	269		MAC	00:1F:45:47:76:35
12.2288.8	ge.1.15	271		MAC	00:1F:45:7A:1B:CC
12.2288.8	ge.1.15	271		MAC	00:1F:45:7A:1B:E7
12.2288.8	ge.1.16	272		MAC	00:11:88:A9:7D:20
12.2288.8	ge.1.17	273		MAC	00:11:88:16:8B:01
12.2288.8	ge.1.18	274		MAC	00:00:12:10:09:08

### Device

The IP address or name of the device.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### Alias

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

### Type

The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is displayed, it signifies that a rule has been applied to the port, overriding the

user's current role with a different role. An example of this would be if the Automated Security Manager has detected a threat on the port, and used a MAC address rule to apply the Quarantine role to the end user.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

### MAC Address

The MAC address of the remote user of this login session.

### IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session. If Anti-Spoofing is enabled and configured, this column displays IP addresses found in the Anti-Spoofing MAC-to-IP address binding table. For more information, see [How to Configure Anti-Spoofing](#).

### Hostname

The hostname of the remote user of this login session. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Port Usage tabs using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

### Current Role

The role under which the user authenticated on the port. If a session displays "Invalid Role" in this column, check the Invalid Role Action setting on the [device Role/Rule tab](#) to see the action that was configured in the event a user is assigned an unknown or invalid role. If the user authenticated via RFC 3580 VLAN Authorization, this column will display the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been configured, the port's Default role will be displayed (if there is one); otherwise, the column will display "N/A."

### Default VLAN ID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

### Default VLAN ID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

### RFC3580 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."

### 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." Use the [Port Properties Authentication Configuration tab](#) to change these settings, if desired.

### Start Time

The time and date when the login session started.

### Duration

The duration of the user's login session, in the format D + HH:MM:SS.



### **Authentication Status**

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

### **Terminate Cause**

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

### **Authentication Server**

The RADIUS server that authenticated the session.

### **Session ID**

A unique identifier for the session. For devices that support multiple authenticated users per port, each user on the port will have a different

session ID. Sessions with an authentication type of MAC or [Role Override](#) will display "N/A."

**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. Devices must be created using SNMPv3 in order to see this value. Devices using SNMPv1 will display "N/A."

**Transmitted Bytes**

The number of bytes transmitted in user data frames on this port during this session. Devices must be created using SNMPv3 in order to see this value. Devices using SNMPv1 will display "N/A."

**Received Frames**

The number of user data frames received on this port during this session.

**Transmitted Frames**

The number of user data frames transmitted on this port during this session.

**Retrieve Button**

Gets the device's port information and displays it in the table.

**Terminate Button**

Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate sessions on frozen ports and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface). See [Terminating a Session](#) for more information.

**Lock MAC Address Button**

Enables [MAC Locking](#) on the selected port(s) (static MAC locking). MAC locking must be enabled on the device in order for it to be enabled on a port.

**Show Only Active Sessions Checkbox**

Select this checkbox to display only active sessions (listed in blue text) in the table.

## Rate Limit Violations Tab

This tab displays information about the rate limit violations for the ports on the device, including the current data being collected for sessions in progress and data from previous sessions. You must click **Retrieve** to display the port information in the tables. For more information, see [Defining Rate Limits](#).

Name	Index	Rate Limit	Generated System Log	Generated Trap	Port Disabled
[12.22.77.33] Port fe.2.4	323	1024 Kb/s	No	No	No

### Name

The port interface name.

### Index

The port index number.

### Rate Limit

The rate limit that has been violated (exceeded).

### Direction

Whether the rate limit is for inbound or outbound traffic.

### Generated System Log

Indicates whether a syslog message was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Generated Trap

Indicates whether an audit trap was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Port Disabled

Indicates whether the port was disabled when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

**Retrieve Button**

Retrieves the most recent rate limit violations information for the ports on the device.

**Clear Button**

Clears the violations table. If port traffic continues to exceed the rate limit, the violations will reappear in the table.

**CEP Usage Tab**

This tab displays information about each CEP connection for the ports on the device, including the date and time the connection was made. For devices that support one CEP connection per port, a connection entry remains in the table until a new connection is made on that port or the system is rebooted.

Refer to the [device Authentication tab \(CEP sub-tab\)](#) for information on enabling and configuring CEP on devices that support it.

Device	Interface Name	Index	CEP Type	Current Role	IP Address
10.10.10.20	fe.2.5	27	Siemens IP Phone	IP Phone Role	10.10.10.22

**Device**

The IP address or name of the device.

**Interface Name**

A description of the port.

**Index**

The index value assigned to the port interface.

**CEP Type**

The CEP product type that has made the connection.

**Current Role**

The assigned role for the CEP connection. Each CEP product type has a role mapped to it. When a CEP connects to the network, the device identifies the CEP type and applies the assigned role. You can map a role for a CEP using the [device Authentication tab \(CEP sub-tab\)](#).

**IP Address**

The IP address of the CEP connecting to the port.

**MAC Address**

The MAC address of the CEP connecting to the port.

**Start Time**

The date and time the connection was made.

**Retrieve Button**

Gets the device's CEP connection information and displays it in the table.

---

**Related Information**

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Devices](#)
- [Defining Rate Limits](#)
- [Authentication Configuration Guide](#)

For information on related windows:

- [Authentication Tab \(Device\)](#)
- [General Tab \(Rate Limit\)](#)

## Port Usage Tab (Device Group/Island)

---

The Port Usage tab displays information related to end user login ([authentication](#)) sessions, rate limit violations, and CEP (Convergence End Point) connections for the devices in a group, a Policy VLAN Island, or a Network Resource Topology Island. To display this tab:

- select a device group in the left-panel Network Elements tab
- select a VLAN island in the left-panel of the Access Control Configuration window (available from the Policy Manager Edit menu)
- select a topology island in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu)

then click the Port Usage tab in the right panel. You must click **Retrieve** to display the port information in the tables.

The Port Usage tab provides three sub-tabs to allow you to view the desired information:

- [End User Sessions Tab](#)
- [Rate Limit Violations Tab](#)
- [CEP Usage Tab](#)

### End User Sessions Tab

This tab displays information about each login session for the ports on the devices in the device group or island, 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. You must click **Retrieve** to display the port information in the table.

By default the **Show Only Active Sessions** checkbox is checked, and only your active sessions are displayed. Deselect the checkbox to display all entries. Active sessions that are being applied to traffic are listed in blue text. Active sessions that are not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type

precedence (configured on the device Authentication tab) determines which type will be applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC,) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports will be listed in the table, along with the roles under which they are authenticated.

Device	Interface Name	Index	Alias	Type	MAC Address
12.2288.1	ge.1.9	265		Auto Tracking	00:1F:45:47:4B:F4
12.2288.1	ge.1.9	265		Auto Tracking	00:1F:45:47:4B:F5
12.2288.1	ge.1.10	266		Auto Tracking	00:01:F4:40:CB:0E
12.2288.1	ge.1.10	266		Auto Tracking	00:11:88:BD:CC:36
12.2288.1	ge.1.11	267		Auto Tracking	00:11:88:FD:91:40
12.2288.1	ge.1.12	268		Auto Tracking	00:11:88:A9:19:A0
12.2288.1	ge.1.13	269		Auto Tracking	00:1F:45:47:76:34
12.2288.1	ge.1.13	269		Auto Tracking	00:1F:45:47:76:35
12.2288.1	ge.1.15	271		Auto Tracking	00:1F:45:7A:1B:CC
12.2288.1	ge.1.15	271		Auto Tracking	00:1F:45:7A:1B:E7
12.2288.1	ge.1.16	272		Auto Tracking	00:11:88:A9:7D:20
12.2288.1	ge.1.17	273		Auto Tracking	00:11:88:16:8B:01

### Device

The IP address or name of the device in the selected device group or island.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### Alias

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

## Type

The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role. An example of this would be if the Automated Security Manager has detected a threat on the port, and used a MAC address rule to apply the Quarantine role to the end user.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

## MAC Address

The MAC address of the remote user of this login session.

## IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session. If Anti-Spoofing is enabled and configured, this column displays IP addresses found in the Anti-Spoofing MAC-to-IP address binding table. For more information, see [How to Configure Anti-Spoofing](#).

## Hostname

The hostname of the remote user of this login session. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Port Usage tabs using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

## Current Role

The role under which the user authenticated on the port. If a session displays "Invalid Role" in this column, check the Invalid Role Action setting on the [device Role/Rule tab](#) to see the action that was configured in the event a user is assigned an unknown or invalid role. If the user authenticated via RFC 3580 VLAN Authorization, this column will display



the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been configured, the port's Default role will be displayed (if there is one); otherwise, the column will display "N/A."

### Default VLAN ID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

### Default VLAN ID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

### RFC3580 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."

### 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." Use the [Port Properties Authentication Configuration tab](#) to change these settings, if desired.

**Start Time**

The time and date when the login session started.

**Duration**

The duration of the user's login session, in the format D + HH:MM:SS.

**Authentication Status**

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

**Terminate Cause**

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

### Authentication Server

The RADIUS server that authenticated the session.

### Session ID

A unique identifier for the session. For devices that support multiple authenticated users per port, each user on the port will have a different session ID. Sessions with an authentication type of MAC or [Role Override](#) will display "N/A."

### 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.

### Transmitted Bytes

The number of bytes transmitted in user data frames on this port during this session.

### Received Frames

The number of user data frames received on this port during this session.

### Transmitted Frames

The number of user data frames transmitted on this port during this session.

### Retrieve Button

Gets the port information for the devices in the device group or island, and displays it in the table.

### Terminate Button

Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate sessions on frozen ports and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface). See [Terminating a Session](#) for more information.

### Lock MAC Address Button

Enables [MAC Locking](#) on the selected port(s) (static MAC locking). MAC locking must be enabled on the device in order for it to be enabled on a port.

### Show Only Active Sessions Checkbox

Select this checkbox to display only active sessions (listed in blue text) in the table.

## Rate Limit Violations Tab

This tab displays information about the rate limit violations for the ports on the devices in the device group or island, including the current data being collected for sessions in progress and data from previous sessions. You must click **Retrieve** to display the port information in the tables. For more information, see [Defining Rate Limits](#).

Name	Index	Rate Limit	Generated System Log	Generated Trap	Port Disabled
[12.22.77.33] Port fe.2/4	323	1024 Kbps	No	No	No

### Name

The port interface name.

### Index

The port index number.

### Rate Limit

The rate limit that has been violated (exceeded).

### Generated System Log

Indicates whether a syslog message was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Generated Trap

Indicates whether an audit trap was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Port Disabled

Indicates whether the port was disabled when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Retrieve Button

Retrieves the most recent rate limit violations information for the ports on the device in the device group or VLAN island.

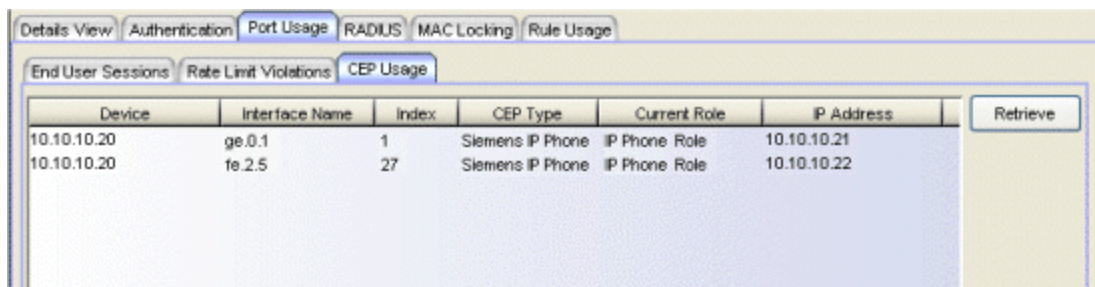
## Clear Button

Clears the violations table. If port traffic continues to exceed the rate limit, the violations will reappear in the table.

## CEP Usage Tab

This tab displays information about each CEP connection for the ports on the devices, including the date and time the connection was made. For devices that support one CEP connection per port, a connection entry remains in the table until a new connection is made on that port or the system is rebooted.

Refer to the [device Authentication tab \(CEP sub-tab\)](#) for information on enabling and configuring CEP on devices that support it.



Device	Interface Name	Index	CEP Type	Current Role	IP Address	Retrieve
10.10.10.20	ge.0.1	1	Siemens IP Phone	IP Phone Role	10.10.10.21	
10.10.10.20	fe.2.5	27	Siemens IP Phone	IP Phone Role	10.10.10.22	

### Device

The IP address or name of the device.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### CEP Type

The CEP product type that has made the connection.

### Current Role

The assigned role for the CEP connection. Each CEP product type has a role mapped to it. When a CEP connects to the network, the device identifies the CEP type and applies the assigned role. You can map a role for a CEP using the [device Authentication tab \(CEP sub-tab\)](#).

### IP Address

The IP address of the CEP connecting to the port.

### MAC Address

The MAC address of the CEP connecting to the port.

**Start Time**

The date and time the connection was made.

**Retrieve Button**

Gets the device group or VLAN island CEP connection information and displays it in the table.

---

**Related Information**

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Devices](#)
- [Defining Rate Limits](#)
- [Authentication Configuration Guide](#)

For information on related windows:

- [Authentication Tab](#)
- [General Tab \(Rate Limit\)](#)

## Port Usage Tab (My Network/All Devices Folder)

---

This Port Usage tab displays information related to end user login ([authentication](#)) sessions, rate limit violations, and CEP (Convergence End Point) connections for all devices in the current domain. To access this tab, select either the My Network or the All Devices folder in the left-panel Network Elements tab, then click the Port Usage tab in the right panel. You must click **Retrieve** to display the port information in the tables.

The Port Usage tab provides three sub-tabs to allow you to view the desired information:

- [End User Sessions Tab](#)
- [Rate Limit Violations Tab](#)
- [CEP Usage Tab](#)

### End User Sessions Tab

This tab displays information about each login session for the ports on the listed 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. You must click **Retrieve** to display the port information in the table.

By default the **Show Only Active Sessions** checkbox is checked, and only your active sessions are displayed. Deselect the checkbox to display all entries. Active sessions that are being applied to traffic are listed in blue text. Active sessions that are not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type will be applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC,) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the

user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

---

**NOTE:** Devices configured for multi-user authentication always list *only* active sessions even if the Show Only Active Session checkbox is deselected.

---

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports will be listed in the table, along with the roles under which they are authenticated.

Device	Interface Name	Index	Alias	Type	MAC Address
12.2288.1	ge.1.9	265		Auto Tracking	00:1F:45:47:4B:F4
12.2288.1	ge.1.9	265		Auto Tracking	00:1F:45:47:4B:F5
12.2288.1	ge.1.10	266		Auto Tracking	00:01:F4:40:CB:0E
12.2288.1	ge.1.10	266		Auto Tracking	00:11:88:BD:CC:36
12.2288.1	ge.1.11	267		Auto Tracking	00:11:88:FD:91:40
12.2288.1	ge.1.12	268		Auto Tracking	00:11:88:A9:19:A0
12.2288.1	ge.1.13	269		Auto Tracking	00:1F:45:47:76:34
12.2288.1	ge.1.13	269		Auto Tracking	00:1F:45:47:76:35
12.2288.1	ge.1.15	271		Auto Tracking	00:1F:45:7A:1B:CC
12.2288.1	ge.1.15	271		Auto Tracking	00:1F:45:7A:1B:E7
12.2288.1	ge.1.16	272		Auto Tracking	00:11:88:A9:7D:20
12.2288.1	ge.1.17	273		Auto Tracking	00:11:88:16:8B:01

### Device

The IP address or name of the device.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### Alias

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

### Type

The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is



displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role. An example of this would be if the Automated Security Manager has detected a threat on the port, and used a MAC address rule to apply the Quarantine role to the end user.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

### MAC Address

The MAC address of the remote user of this login session.

### IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session. If Anti-Spoofing is enabled and configured, this column displays IP addresses found in the Anti-Spoofing MAC-to-IP address binding table. For more information, see [How to Configure Anti-Spoofing](#).

### Hostname

The hostname of the remote user of this login session. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Port Usage tabs using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

### Current Role

The role under which the user authenticated on the port. If a session displays "Invalid Role" in this column, check the Invalid Role Action setting on the [device Role/Rule tab](#) to see the action that was configured in the event a user is assigned an unknown or invalid role. If the user authenticated via RFC 3580 VLAN Authorization, this column will display the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been

configured, the port's Default role will be displayed (if there is one); otherwise, the column will display "N/A."

### Default VLAN ID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

### Default VLAN ID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

### RFC3580 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."

### 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." Use the [Port Properties Authentication Configuration tab](#) to change these settings, if desired.

### Start Time

The time and date when the login session started.

### **Duration**

The duration of the user's login session, in the format D + HH:MM:SS.

### **Authentication Status**

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

### **Terminate Cause**

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

### **Authentication Server**

The RADIUS server that authenticated the session.

### Session ID

A unique identifier for the session. For devices that support multiple authenticated users per port, each user on the port will have a different session ID. Sessions with an authentication type of MAC or [Role Override](#) will display "N/A."

### 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.

### Transmitted Bytes

The number of bytes transmitted in user data frames on this port during this session.

### Received Frames

The number of user data frames received on this port during this session.

### Transmitted Frames

The number of user data frames transmitted on this port during this session.

### Retrieve Button

Gets the port information for the devices, and displays it in the table.

### Terminate Button

Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate sessions on frozen ports and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface). See [Terminating a Session](#) for more information.

### Lock MAC Address Button

Enables [MAC Locking](#) on the selected port(s) (static MAC locking). MAC locking must be enabled on the device in order for it to be enabled on a port.

### Show Only Active Sessions Checkbox

Select this checkbox to display only active sessions (listed in blue text) in the table.

## Rate Limit Violations Tab

This tab displays information about the rate limit violations for the ports on all devices, including the current data being collected for sessions in progress and data from previous sessions. You must click **Retrieve** to display the port information in the tables. For more information, see [Defining Rate Limits](#).

Name	Index	Rate Limit	Generated System Log	Generated Trap	Port Disabled
[12.22.77.33] Port fe.2.4	323	1024 Kbps	No	No	No

### Name

The port interface name.

### Index

The port index number.

### Rate Limit

The rate limit that has been violated (exceeded).

### Generated System Log

Indicates whether a syslog message was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Generated Trap

Indicates whether an audit trap was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Port Disabled

Indicates whether the port was disabled when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Retrieve Button

Retrieves the most recent rate limit violations information for the ports on all devices.

## Clear Button

Clears the violations table. If port traffic continues to exceed the rate limit, the violations will reappear in the table.

## CEP Usage Tab

This tab displays information about each CEP connection for the ports on the devices, including the date and time the connection was made. For devices that support one CEP connection per port, a connection entry remains in the table until a new connection is made on that port or the system is rebooted.

Refer to the [device Authentication tab \(CEP sub-tab\)](#) for information on enabling and configuring CEP on devices that support it.

Device	Interface Name	Index	CEP Type	Current Role	IP Address
10.10.10.20	ge.0.1	1	Siemens IP Phone	IP Phone Role	10.10.10.21
10.10.10.20	fe.2.5	27	Siemens IP Phone	IP Phone Role	10.10.10.22

### Device

The IP address or name of the device.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### CEP Type

The CEP product type that has made the connection.

### Current Role

The assigned role for the CEP connection. Each CEP product type has a role mapped to it. When a CEP connects to the network, the device identifies the CEP type and applies the assigned role. You can map a role for a CEP using the [device Authentication tab \(CEP sub-tab\)](#).

### IP Address

The IP address of the CEP connecting to the port.

### MAC Address

The MAC address of the CEP connecting to the port.

**Start Time**

The date and time the connection was made.

**Retrieve Button**

Gets the device group CEP connection information and displays it in the table.

---

**Related Information**

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Devices](#)
- [Defining Rate Limits](#)
- [Authentication Configuration Guide](#)

For information on related windows:

- [Authentication Tab](#)
- [General Tab \(Rate Limit\)](#)

## Port Usage Tab (Port Group)

---

The Port Usage tab displays information related to end user login ([authentication](#)) sessions, rate limit violations, and CEP (Convergence End Point) connections for the ports in the selected port group. To display this tab, select a port group in the left-panel Port Groups tab and the Port Usage tab in the right panel. You must click **Retrieve** to display the port information in the tables.

The Port Usage tab provides three sub-tabs to allow you to view the desired information:

- [End User Sessions Tab](#)
- [Rate Limit Violations Tab](#)
- [CEP Usage Tab](#)

### End User Sessions Tab

This tab displays login session information for each port in the selected port group, 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. You must click **Retrieve** to display the port information in the table.

By default the **Show Only Active Sessions** checkbox is checked, and only your active sessions are displayed. Deselect the checkbox to display all entries. Active sessions that are being applied to traffic are listed in blue text. Active sessions that are not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type will be applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC,) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is



disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

**NOTE:** Devices configured for multi-user authentication always list *only* active sessions even if the Show Only Active Session checkbox is deselected.

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports will be listed in the table, along with the roles under which they are authenticated.

Device	Interface Name	Index	Alias	Type	MAC Address
122288.8	ge.1.10	266		MAC	00:01:F4:40:CB:0E
122288.8	ge.1.10	266		MAC	00:11:88:BD:CC:36
122288.8	ge.1.11	267		MAC	00:11:88:FD:91:40
122288.8	ge.1.12	268		MAC	00:11:88:A9:19:A0
122288.8	ge.1.13	269		MAC	00:1F:45:47:76:34
122288.8	ge.1.13	269		MAC	00:1F:45:47:76:35
122288.8	ge.1.15	271		MAC	00:1F:45:7A:1B:CC
122288.8	ge.1.15	271		MAC	00:1F:45:7A:1B:E7
122288.8	ge.1.16	272		MAC	00:11:88:A9:7D:20
122288.8	ge.1.17	273		MAC	00:11:88:16:68:01
122288.8	ge.1.18	274		MAC	00:00:12:10:09:08
122288.8	ge.1.19	275		MAC	00:11:88:72:2C:00
122288.8	ge.1.21	277		MAC	00:0C:29:6F:DC:DC

### Device

The IP address or name of the device where the port is located.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### Alias

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

### Type

The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is

displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role. An example of this would be if the Automated Security Manager has detected a threat on the port, and used a MAC address rule to apply the Quarantine role to the end user.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

### MAC Address

The MAC address of the remote user of this login session.

### IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session. If Anti-Spoofing is enabled and configured, this column displays IP addresses found in the Anti-Spoofing MAC-to-IP address binding table. For more information, see [How to Configure Anti-Spoofing](#).

### Hostname

The hostname of the remote user of this login session. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Port Usage tabs using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

### Current Role

The role under which the user authenticated on the port. If a session displays "Invalid Role" in this column, check the Invalid Role Action setting on the [device Role/Rule tab](#) to see the action that was configured in the event a user is assigned an unknown or invalid role. If the user authenticated via RFC 3580 VLAN Authorization, this column will display the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been

configured, the port's Default role will be displayed (if there is one); otherwise, the column will display "N/A."

### Default VLAN ID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

### Default VLAN ID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

### RFC3580 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."

### 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." Use the [Port Properties Authentication Configuration tab](#) to change these settings, if desired.

### Start Time

The time and date when the login session started.

### **Duration**

The duration of the user's login session, in the format D + HH:MM:SS.

### **Authentication Status**

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

### **Terminate Cause**

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

### **Authentication Server**

The RADIUS server that authenticated the session.

**Session ID**

A unique identifier for the session. For devices that support multiple authenticated users per port, each user on the port will have a different session ID. Sessions with an authentication type of MAC or [Role Override](#) will display "N/A."

**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.

**Transmitted Bytes**

The number of bytes transmitted in user data frames on this port during this session.

**Received Frames**

The number of user data frames received on this port during this session.

**Transmitted Frames**

The number of user data frames transmitted on this port during this session.

**Retrieve Button**

Reads the latest information about the port group and displays it in the table.

**Terminate Button**

Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate sessions on frozen ports and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface). See [Terminating a Session](#) for more information.

**Lock MAC Address Button**

Enables [MAC Locking](#) on the selected port(s) (static MAC locking). MAC locking must be enabled on the device in order for it to be enabled on a port.

**Show Only Active Sessions Checkbox**

Select this checkbox to display only active sessions (listed in blue text) in the table.

## Rate Limit Violations Tab

These tables displays information about the rate limit violations for the ports in the selected port group, including the current data being collected for sessions in progress and data from previous sessions. You must click **Retrieve** to display the port information in the tables. For more information, see [Defining Rate Limits](#).

Name	Index	Rate Limit	Generated System Log	Generated Trap	Port Disabled
[12.22.77.33] Port fe.2.4 323	323	1024 Kbps	No	No	No
[12.22.77.34] Port fe.2.2 322	322	1024 Kbps	No	No	No

### Name

The port interface name.

### Index

The port index number.

### Rate Limit

The rate limit that has been violated (exceeded).

### Generated System Log

Indicates whether a syslog message was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Generated Trap

Indicates whether an audit trap was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

### Port Disabled

Indicates whether the port was disabled when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

**Retrieve Button**

Retrieves the most recent rate limit violations information for the ports in the selected port group.

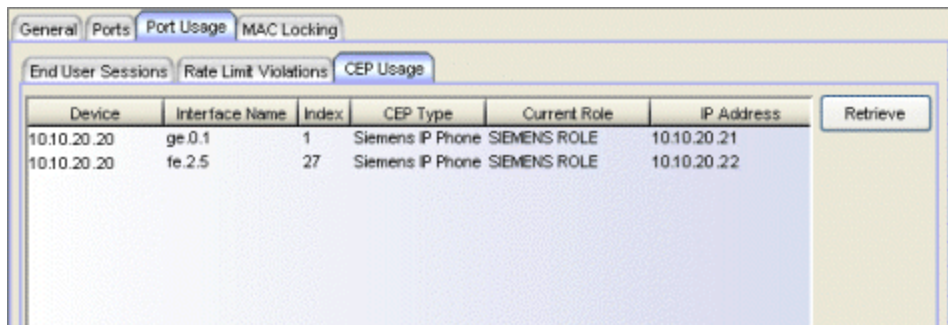
**Clear Button**

Clears the violations table. If port traffic continues to exceed the rate limit, the violations will reappear in the table.

**CEP Usage Tab**

The table displays information about any CEP connection for the ports in the group, including the date and time the connection was made. For devices that support one CEP connection per port, a connection entry remains in the table until a new connection is made on that port or the system is rebooted.

Refer to the [device Authentication tab \(CEP sub-tab\)](#) for information on enabling and configuring CEP on devices that support it.



Device	Interface Name	Index	CEP Type	Current Role	IP Address
10.10.20.20	ge.0.1	1	Siemens IP Phone	SIEMENS ROLE	10.10.20.21
10.10.20.20	fe.2.5	27	Siemens IP Phone	SIEMENS ROLE	10.10.20.22

**Device**

The IP address or name of the device where the port is located.

**Interface Name**

A description of the port.

**Index**

The index value assigned to the port interface.

**CEP Type**

The CEP product type.

**Current Role**

The assigned role for the CEP connection. Each CEP product type has a role mapped to it. When a CEP connects to the network, the device identifies the CEP type and applies the assigned role. You can map a role for a CEP using the [device Authentication tab \(CEP sub-tab\)](#).

**IP Address**

The IP address of the CEP connecting to the port.

**MAC Address**

The MAC address of the CEP connecting to the port.

**Start Time**

The date and time the connection was made.

**Retrieve Button**

Gets the port group CEP connection information and displays it in the table.

---

**Related Information**

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Ports](#)
- [Defining Rate Limits](#)
- [Authentication Configuration Guide](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)



## Precedence Tab (Rate Limits Folder)

---

The Precedence tab is for legacy devices only. It enables you to set the order in which priority-based rate limits will be written to devices that support them.

Policy Manager allows you to define as many rate limits as you wish; however, the number written to a device is restricted by the number of rate limits supported by the device. Rate limits will be written to a device in the order displayed on this tab, up until the maximum number of rate limits has been reached on each device. Rate limits are listed in the order of precedence under the rate limit folder in the left-panel tree.

---

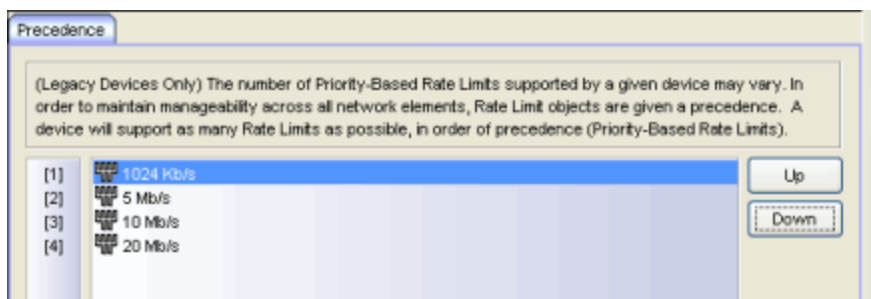
**NOTE:** Although all rate limits have a precedence and show up in this list, only rate limits that include a priority-based configuration will actually be written to a device.

---

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select the Rate Limits folder in the tree, and the Precedence tab will display in the right panel.

This tab also appears when you select the Precedence **Edit** button on the Rate Limit [General tab](#).

The Precedence tab lists all the currently defined rate limits and their current precedence. To use the Precedence tab, select the rate limit you want to position, and use the **Up** or **Down** button to move it to the desired place in the list.



---

### Related Information

For information on related concepts:

- [Priority-Based Rate Limits](#)

For information on related tasks:

- [How to Define Priority-Based Rate Limits](#)

## RADIUS Tab (Device)

The device RADIUS tab allows you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and Policy Manager, for the purposes of [authentication](#) and accounting (for your SNMPv3 devices that support it).

RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. It is used by a device to save accounting data on a RADIUS server. Accounting requests are sent from the device to the server. The server acknowledges these requests, and data is passed to the server via accounting updates. For more information on accounting functionality, refer to your RADIUS server documentation.

To display the device RADIUS tab, select a device in the left-panel Network Elements tab, then click the RADIUS tab in the right panel.

The screenshot displays the RADIUS configuration interface with two main sections: Client Settings and RADIUS Server(s).

**Client Settings:**

- Authentication Status: Disabled
- Management Access Auth Status Override: Disabled
- Network Access Auth Status Override: Disabled
- Number of Retries: 2
- Timeout Duration (seconds): 5
- Management Access Timeout Duration Override (sec): N/A
- Network Access Timeout Duration Override (sec): N/A
- Response Mode: Filter ID (Discard VTA)
- Retransmit Algorithm: Standard
- Application Shared Secret (Legacy): Change shared secret: Select...

**RADIUS Server(s):**

NOTE: Legacy priority entries take higher precedence than all other servers.

Priority	RADIUS Server Address	Client UDP Port	Access Type	Current Sessions	Max Sessions	Number of Retries	Timeout Duration (sec)	Mgmt Interface
Mgmt Secondary (Legacy)		1812	Any access	--	--	Client Default	Client Default	N/A
Netlogn Primary (Legacy)	134.141.104.86	1812	Network access	--	--	Client Default	Client Default	N/A
Netlogn Secondary (Legacy)	134.141.104.87	1812	Network access	--	--	Client Default	Client Default	N/A

## Authentication Tab

Use this tab to view and configure the RADIUS authentication servers with which the device (the RADIUS client) can communicate.

### *RADIUS Authentication Client Settings*

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS authentication servers, and specify connection attempt information.

#### **Authentication Status**

Allows you to enable and disable communication between this device and the RADIUS authentication server(s). If enabled, the device becomes a RADIUS client and will communicate with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS authentication server (see the [Authentication Configuration Guide](#)). The default is Disabled. For ExtremeWireless Wireless devices, the Client Status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not.

#### **Management Access Auth Status Override**

Allows you to override the Authentication Status for users accessing the RADIUS authentication server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

#### **Network Access Auth Status Override**

Allows you to override the Authentication Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

#### **Number of Retries**

The number of attempts the device will make in contacting each RADIUS authentication server before giving up and trying the next RADIUS authentication server on the list. Valid values are 1-65535. For ExtremeWireless Wireless devices, this value is entered when the RADIUS server is added.

#### **Timeout Duration**

The total number of seconds the device will wait for the RADIUS authentication server to respond, before trying again. Valid values are 1-65535. For ExtremeWireless Wireless devices, this value is entered when the RADIUS server is added.

**Management Access Timeout Duration Override (sec)**

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the RADIUS authentication server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

**Network Access Timeout Duration Override (sec)**

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

**Response Mode**

Select the RADIUS response attribute that the device should use for authentication:

- **Filter ID** — The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it will be ignored.
- **VLAN Tunnel Attribute** — The VLAN Tunnel Attribute is used and the [Authentication-Based VLAN to Role Mappings](#) are applied, if present. If a Filter ID is returned, it will be ignored.
- **Filter ID With VLAN Tunnel Attribute** — Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel Attribute replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

**Retransmit Algorithm**

Select the authentication retransmission algorithm for this device to use with your RADIUS servers. Devices that do not support this functionality will have the option grayed out.

- **Standard** — Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable due to a network outage or because server capacity is exceeded.
- **Round-Robin** — The round-robin RADIUS authentication algorithm spreads RADIUS server usage evenly between available RADIUS servers, allowing the load balancing of a large number of authentications across all RADIUS servers. This allows for a maximum authentication throughput for

the number of servers configured. Additionally, if a single server is down, only a portion of the authenticating sessions will be affected by the outage.

- **Sticky Round-Robin** — This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server should be used for any given authentication session once a session is initiated. In large-scale NAC deployments, this algorithm is used for switches that are authenticating more users than a NAC appliance supports. For example, a NAC deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three NAC appliances that support 3000 users each. In this scenario, the sticky round-robin algorithm allows the S-Series device to spread the load across all three NAC appliances while using the same NAC appliance for all RADIUS transactions for a given session (MAC address).

### Apply Button

Applies the changes you made in the RADIUS Authentication Client Settings section.

### Application Shared Secret (Legacy)

The device (the RADIUS client) and Policy Manager share a common "secret" that provides for a secure means of RADIUS client configuration on devices using SNMPv1. This "Application Shared Secret" is a string of characters used to encrypt and decrypt communication between Policy Manager and the device. A Default shared secret is provided that allows you to initially configure the RADIUS settings on this tab, but it is recommended that you change this secret to increase security.

Click the **Change** button to make the Application Shared Secret fields available for editing and select the method for changing the string:

- **Auto-Generated** — Generates a new 32-character Application Shared Secret automatically.
- **User-Defined** — Enter a new shared secret in the field. The format is a 32-character string with optional dashes or spaces, typically xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx.
- **Default** — Uses the default shared secret that is provided to allow you to initially configure the RADIUS settings on this tab. It is recommended that you change to an auto-generated or user-defined secret to increase security.

Click the **Apply** button to save any changes you made.

---

**NOTE:** This Application Shared Secret is not to be confused with the Server Shared Secret that encrypts communication between the RADIUS server and the RADIUS client, entered in the [Add RADIUS Authentication Server window](#) or [Add RADIUS Accounting Server window](#) available from the **Add** buttons on this tab, or in the [Add RADIUS Server window](#) in the Device Configuration Wizard.

---

**WARNING:** It is important to remember the Application Shared Secret, since the shared secret specified in Policy Manager must match the shared secret on the device. If you delete and recreate the device in Policy Manager, you will have to supply the correct Application Shared Secret in the device's RADIUS tab in order to retrieve or input the RADIUS settings on this tab. If you're using an Auto-Generated or User-Defined Application Shared Secret and you clear NVRAM on the device, you will need to go to the RADIUS tab for the device and change the Application Shared Secret back to "Default" in order to regain access to the RADIUS information in that tab. Once Policy Manager and the device are using the same (Default) Application Shared Secret, then the secret can be changed to be either Auto-Generated or User-Defined.

---

### *Authentication RADIUS Server(s) Table*

This table lists the RADIUS authentication servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

#### **Priority**

Order in which the RADIUS authentication server is checked, as compared to the other RADIUS authentication servers listed here. The lower the number, the higher the priority.

#### **RADIUS Server IP**

IP address of the RADIUS authentication server.

#### **Client UDP Port**

UDP port number (1-65535) on the RADIUS authentication server that the device will send authentication requests to; 1812 is the default port number.

#### **Access Type**

The type of authentication access allowed for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.

- **Network access** — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication. Devices that do not support this feature will display N/A in this column.

### Current Sessions

The current number of sessions associated with this server when the device is using the [sticky round-robin RADIUS authentication algorithm](#). This value is not used when other algorithms are being used.

### Max Sessions

The maximum number of sticky round-robin authentication sessions allowed on the server when the [sticky round-robin RADIUS authentication algorithm](#) is configured for the device. This value is not used when other algorithms are being used. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to.

### Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section.

### Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section.

### Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

### Apply Button

Applies any changes you made in the RADIUS Authentication Server(s) tab.



## Add Button

Opens the [Add RADIUS Authentication Server window](#), where you can enter the parameters for a server you want to add to the list. When you click **OK** on this window, the new server is added.

## Remove Button

Select a RADIUS authentication server in the list and use this button to remove the server.

## Edit Button

Select a RADIUS authentication server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

## Accounting Tab

Use this tab to view and configure the RADIUS accounting servers with which the device (the RADIUS client) can communicate.

Details View | Ports | General | Role/Rule | Authentication | Port Usage | **RADIUS** | Anti-Spoofing | MAC Locking | Rule Usage

Authentication | **Accounting** | Port Configuration

**Client Settings**

Accounting Status: Disabled

Management Access Auth Status Override: Disabled

Network Access Auth Status Override: Disabled

Quarantine Accounting Status: Disabled

802.1X Accounting Status: Disabled

PWA Accounting Status: Disabled

MAC Accounting Status: Disabled

CEP Accounting Status: Disabled

Auto Tracking Accounting Status: Disabled

Update Interval (minutes): 0

Management Access Timeout Duration (sec): N/A

Network Access Timeout Duration (sec): N/A

Apply

**RADIUS Server(s)**

NOTE: Legacy priority entries take higher precedence than all other servers.

Priority	RADIUS Server IP	Client UDP Port	Access Type	Number of Retries	Timeout Duration (sec)	Update Interval (min)	
Netlogon Primary (Legacy)	134.141.104.86	1813	N/A	3	Client Default	Client Default	N/A
Netlogon Secondary (Legacy)	134.141.104.87	1813	N/A	3	Client Default	Client Default	N/A

Apply

Add...

Remove

Edit...

## *RADIUS Accounting Client Settings*

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS accounting servers, and specify the update interval.

### **Accounting Status**

Allows you to enable or disable RADIUS accounting on SNMPv3 devices that support it. RADIUS accounting is used by a device to save accounting data on a RADIUS accounting server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server. The default is Disabled. For ExtremeWireless Wireless devices, the status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. Devices that do not support RADIUS accounting will have this field grayed out.

### **Management Access Auth Status Override**

Allows you to override the Accounting Status for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

### **Network Access Auth Status Override**

Allows you to override the Accounting Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

### **Per Authentication Type Accounting Status**

Allows you to enable/disable RADIUS accounting for individual authentication types. Some authentication types do not have RADIUS accounting enabled by default (when global RADIUS accounting is enabled). Enabling these authentication types will give both NAC and other RADIUS servers more complete information regarding authentication sessions. These options also allow you to disable accounting messages from certain authentication types, for example, Auto-Tracking, which does not actually authenticate end users. Note that the global [Accounting Status](#) option controls accounting on a global basis for all authentication types. Devices that do not support this functionality will have these fields grayed out.

### **Update Interval (minutes)**

Collected accounting data is sent from the device to the RADIUS accounting server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Valid values

are 1-65535. It is recommended that the value be greater than 10 minutes, and careful consideration should be given to its impact on network traffic. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.) For ExtremeWireless Wireless devices, this value is entered when the RADIUS server is added.

**Management Access Timeout Duration Override (sec)**

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

**Network Access Timeout Duration Override (sec)**

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

**Apply Button**

Applies the changes you made in the RADIUS Accounting Client Settings section.

*Accounting RADIUS Servers Table*

This tab lists the RADIUS accounting servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

**Priority**

Order in which the RADIUS accounting server is checked, as compared to the other RADIUS accounting servers listed here. The lower the number, the higher the priority.

**RADIUS Server IP**

IP address of the RADIUS accounting server.

**Client UDP Port**

UDP port number (1-65535) on the RADIUS accounting server that the device will send accounting requests to; 1813 is the default port number. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Access Type

The type of authentication access allowed for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature will display N/A in this column.

### Number of Retries

The number of times the device will resend an accounting request if the RADIUS accounting server does not respond. Valid values are 0-20.

Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Timeout Duration

The amount of time in seconds the device will wait for the RADIUS accounting server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Update Interval

The amount of time in minutes between accounting updates. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Accounting Client Settings](#) section.

### Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

### Apply Button

Applies any changes you made in the RADIUS Accounting Server(s) tab.

### Add Button

Opens the [Add RADIUS Accounting Server window](#), where you can enter the parameters for a server you want to add to the list. When you click **OK** on this window, the new server is added.

## Remove Button

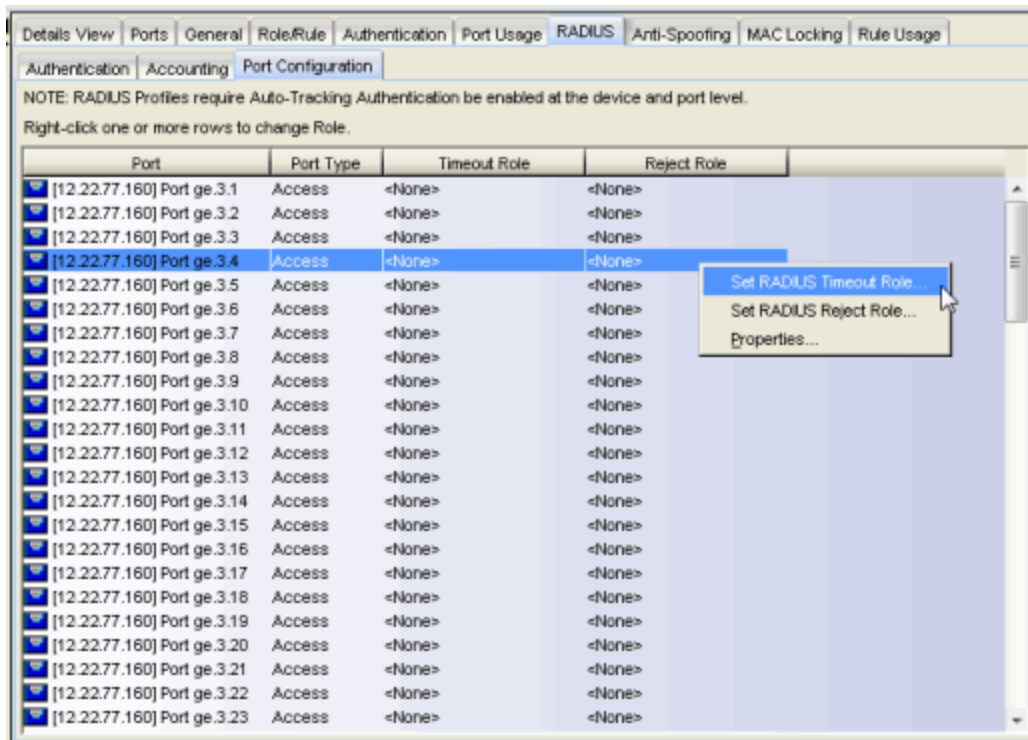
Select a RADIUS accounting server in the list and use this button to remove the server.

## Edit Button

Select a RADIUS accounting server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

## Port Configuration Tab

This tab displays all the ports on the device and allows you to configure the [RADIUS Timeout role](#) and the [RADIUS Reject Role](#) for one or more ports via a right-click menu. It also provides access to the Port Properties window for a single port.



## Related Information

For information on related concepts:

- [Authentication](#)

For information on related windows:

- [Port Properties - Authentication Configuration Tab](#)
- [Add RADIUS Authentication Server Window](#)
- [Add RADIUS Accounting Server Window](#)

For information on related tasks:

- [How to Configure Devices](#)
- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

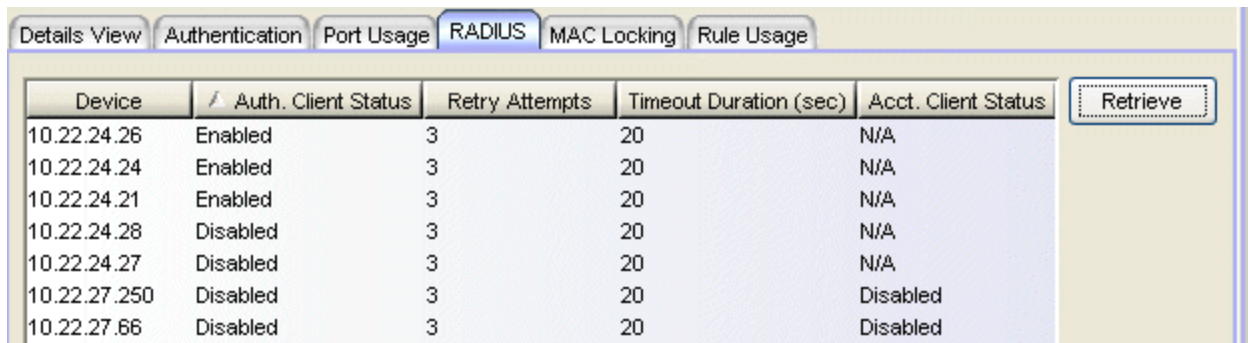
## RADIUS Tab (Device Group/Island)

The RADIUS tab displays authentication and accounting RADIUS server information for all the devices in a device group, a Policy VLAN Island, or a Network Resource Topology Island. You can configure RADIUS server information for a device using the [device's RADIUS Tab](#) or the [Device Configuration Wizard](#).

To access this tab:

- select a device group in the left-panel Network Elements tab
- select a VLAN island in the left-panel of the Access Control Configuration window (available from the Policy Manager Edit menu)
- select a topology island in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu)

then select the RADIUS tab in the right panel.



The screenshot shows a software interface with several tabs: Details View, Authentication, Port Usage, RADIUS (selected), MAC Locking, and Rule Usage. Below the tabs is a table with the following columns: Device, Auth. Client Status, Retry Attempts, Timeout Duration (sec), and Acct. Client Status. A 'Retrieve' button is located to the right of the table.

Device	Auth. Client Status	Retry Attempts	Timeout Duration (sec)	Acct. Client Status
10.22.24.26	Enabled	3	20	N/A
10.22.24.24	Enabled	3	20	N/A
10.22.24.21	Enabled	3	20	N/A
10.22.24.28	Disabled	3	20	N/A
10.22.24.27	Disabled	3	20	N/A
10.22.27.250	Disabled	3	20	Disabled
10.22.27.66	Disabled	3	20	Disabled

### Device

Name or IP address of the device.

### Auth. Client Status

Informs you whether or not the device is enabled as a RADIUS client. If Enabled, the device is a RADIUS client and will communicate with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication. If Disabled, the device is currently not enabled as a RADIUS client.

### Retry Attempts

Number of attempts the device (RADIUS client) will make to connect to the RADIUS authentication server before giving up and trying the next RADIUS server on the list. Valid values are 1-65535.

### Timeout Duration (sec)

Total number of seconds the device (RADIUS client) will wait for the RADIUS authentication server to respond, before trying again. Valid values are 1-65535.

### Acct. Client Status

Informs you whether or not RADIUS accounting is enabled on the device (the RADIUS client). RADIUS accounting is supported on certain SNMPv3 devices, and is used by the device to save accounting data on a RADIUS server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS server. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display a status.)

### Acct. Update Interval (minutes)

Collected accounting data is sent from the device (RADIUS client) to the RADIUS server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display a value.)

### RADIUS Server List

Lists the IP addresses of the RADIUS servers the client device will attempt to contact, followed by the UDP port number used to send authentication requests and the UDP port number used to send accounting requests. The addresses are listed in the order of priority in which the RADIUS server will be contacted. Devices that do not support RADIUS accounting will display N/A for an accounting port (with the exception of an SNMPv1 R2 device, which will display a value.)

### RADIUS Response Mode

Indicates the RADIUS response attribute that the device will use for authentication. You can configure the Response Mode in the [RADIUS tab](#) for the device.

### Retrieve Button

Retrieves the latest RADIUS server information from the devices and displays it in the table.

---

## Related Information

For information on related concepts:



- [Authentication](#)

For information on related windows:

- [Add RADIUS Authentication Server Window](#)
- [Add RADIUS Accounting Server Window](#)
- [Authentication Configuration Tab](#)

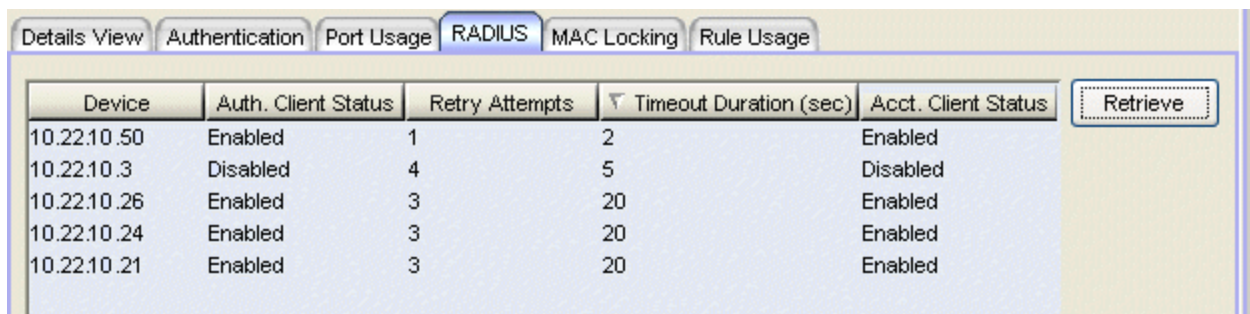
For information on related tasks:

- [How to Configure Devices](#)
- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

## RADIUS Tab (My Network/All Devices Folder)

This RADIUS tab displays authentication and accounting RADIUS server information for all the devices in the current domain. You can configure RADIUS server information for an individual device using the [device's RADIUS Tab](#) or the [Device Configuration Wizard](#).

To access this tab, select either the My Network or the All Devices folder in the left-panel Network Elements tab, then click the RADIUS tab in the right panel. You must click **Retrieve** to display the RADIUS information in the table.



The screenshot shows a software interface with several tabs: Details View, Authentication, Port Usage, RADIUS (selected), MAC Locking, and Rule Usage. Below the tabs is a table with the following data:

Device	Auth. Client Status	Retry Attempts	Timeout Duration (sec)	Acct. Client Status	Retrieve
10.22.10.50	Enabled	1	2	Enabled	<input type="button" value="Retrieve"/>
10.22.10.3	Disabled	4	5	Disabled	
10.22.10.26	Enabled	3	20	Enabled	
10.22.10.24	Enabled	3	20	Enabled	
10.22.10.21	Enabled	3	20	Enabled	

### Device

Name or IP address of the device.

### Auth. Client Status

Informs you whether or not the device is enabled as a RADIUS client. If Enabled, the device is a RADIUS client and will communicate with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication. If Disabled, the device is currently not enabled as a RADIUS client.

### Retry Attempts

Number of attempts the device (RADIUS client) will make to connect to the RADIUS authentication server before giving up and trying the next RADIUS server on the list. Valid values are 1-65535.

### Timeout Duration (sec)

Total number of seconds the device (RADIUS client) will wait for the RADIUS authentication server to respond, before trying again. Valid values are 1-65535.

### Acct. Client Status

Informs you whether or not RADIUS accounting is enabled on the device (the RADIUS client). RADIUS accounting is supported on certain SNMPv3 devices, and is used by the device to save accounting data on a RADIUS server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS server. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display a status.)

### Acct. Update Interval (minutes)

Collected accounting data is sent from the device (RADIUS client) to the RADIUS server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display a value.)

### RADIUS Server List

Lists the IP addresses of the RADIUS servers the client device will attempt to contact, followed by the UDP port number used to send authentication requests and the UDP port number used to send accounting requests. The addresses are listed in the order of priority in which the RADIUS server will be contacted. Devices that do not support RADIUS accounting will display N/A for an accounting port (with the exception of an SNMPv1 R2 device, which will display a value.)

### Response Response Mode

Indicates the RADIUS response attribute that the device will use for authentication. You can configure the Response Mode in the [RADIUS tab](#) for the device.

### Retrieve Button

Retrieves the latest RADIUS server information from the devices and displays it in the table.

---

## Related Information

For information on related concepts:

- [Authentication](#)

For information on related windows:

- [Add RADIUS Authentication Server Window](#)
- [Add RADIUS Accounting Server Window](#)

For information on related tasks:

- [How to Configure Devices](#)
- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

## Role/Rule Tab (Device)

The device Role/Rule tab lets you configure invalid role action and a device-level role (Matrix C1 devices only) for the selected device. It also lets you enable and configure Rule Accounting on devices that support it, and view any ports on the device that have been disabled due to rule usage. To access this tab, select a device on the left panel's Network Elements tab and click the Role/Rule tab in the right panel.

The screenshot shows the configuration interface for the Role/Rule tab. It includes the following sections:

- Invalid Role Action:** Radio buttons for  Apply Default,  Deny Traffic, and  Permit Traffic. Invalid Roles Detected: 1.
- Device Level Role (Matrix C1 Devices Only):** Device Level Role: <None> with a Select... button.
- Rule Accounting / Rule Hit Reporting:** Radio buttons for Rule Accounting (Enabled/Disabled), Use Expanded Format for Rule Hit System Log Messages (Enabled/Disabled), Clear Rule Usage on Port Link-Status Change (Enabled/Disabled), and Clear Rule Usage on Role Mapping Change (Enabled/Disabled). A checkbox for Enable Syslog Server (Policy Reporting) is checked.
- Clear Rule Usage on Interval:** Radio buttons for Enabled (selected) and Disabled. An Apply button is present.
- Interval (minutes):** A text input field containing the value 30.
- Rule Usage Auto Clear Ports:** A list of ports: [10.20.77.33] Port fe.1.1, [10.20.77.33] Port fe.1.2, [10.20.77.33] Port fe.1.3, [10.20.77.33] Port fe.1.4, and [10.20.77.33] Port fe.1.5. Buttons for Add/Remove..., Remove, and Apply are provided.
- Disabled Ports (Rule / Rate Limit Hit):** A table with columns for Port, Index, and Disable Cause. Buttons for Retrieve and Clear are located to the right of the table.

### Invalid Role Action

For devices that support this feature, this area of the tab lets you specify what happens to a user that gets an unknown or invalid role.

### Invalid Role Action

Select the action you would like taken if an authenticated user is assigned an unknown or invalid role:

- Apply Default - Apply the port's default role to the user.
- Deny Traffic - Drop the packets for this user.
- Permit Traffic - Forward traffic with the port's assigned VID.

### Invalid Roles Detected

Displays the number of invalid roles that were found.

## Device Level Role (C1 Devices Only)

On C1 devices, you can set a device-level role that configures the services and rules for all ports on the device. Due to a limitation of the C1 devices, services and rules from the role returned from authentication cannot be applied to the port. The services and rules from this device-level role will be used instead.

### Device Level Role

Displays the device-level role currently set on the device.

### Select

Opens the [Selection View \(Roles\) window](#) where you can select a role to be the device-level role on the device.

## Rule Accounting / Rule Hit Reporting

Rule accounting and rule hit reporting provide the ability to collect data on how policy rules are being used on your network. Use this section to enable rule accounting and configure rule accounting and reporting parameters for this device. Once you have configured the accounting and reporting functionality, you can view the rule usage data that is collected using the Rule Usage tabs or the Policy Rule Hit Reports. On devices that do not support rule accounting, this section will be grayed out. For more information on configuring rule accounting and reporting, and viewing rule usage data, see [Rule Accounting and Rule Hit Reporting](#).

### Rule Accounting

Select whether to enable or disable Rule Accounting on the device.

### Use Expanded Format for Rule Hit System Log Messages

When enabled, the device will provide additional information in Policy Rule Hit syslog messages. For example, the additional information may include

---

what actions may have been initiated by the rule (if any).

---

**NOTE:** Rule accounting is used to show if a given rule has been used to classify traffic on a device, and on which port the rule hit occurred. When a rule is used on a port, an entry is made in the rule hit table. Subsequent rule hits do not alter this entry in the rule hit table, however you can use the "clear rule usage" options discussed below to customize the table to indicate how recently, or in what context, these rule hits have occurred. You can specify that a rule hit is cleared when the port link-status changes, when the role which defines the rule is assigned via a Role Mapping, and/or according to a set interval. Based on these options, you can determine how fresh your rule hit data is, and/or what the rule hit data is within a specific session. For example, if you specify a clear rule usage interval of 30 minutes, then you know that any rule hits displayed in the Rule Usage tab (after you click Retrieve) have been reported in the last 30 minutes. These clear rule usage options also control the frequency that the syslog messages containing the rule hit data are sent from the device for rule hit reporting.

---

#### Clear Rule Usage on Port Link-Status Change

When enabled, this option clears rule usage data when the port has a link-status change when a user connects or disconnects. Ports must be listed in the Rule Usage Auto Clear Ports list (below) to be subject to this clear operation.

#### Clear Rule Usage on Role Mapping Change

If a role-mapping is defined and traffic comes onto the device and is mapped to the defined role, then all rules in that role will have their rule hit data cleared. This option should be enabled for Policy Rule Hit Reporting. It allows you to start a new data collection when the name of the role changes on the port, providing for a cleaner data presentation. Ports must be listed in the Rule Usage Auto Clear Ports list (below) to be subject to this clear operation.

#### Enable Syslog Server

When configuring Policy Rule Hit Reporting, select the **Enable Syslog Server** checkbox to set up the device to send syslog messages.

#### Clear Rule Usage on Interval

When enabled, this option clears the rule usage data at a set interval. This option should be enabled for Policy Rule Hit Reporting because it specifies the interval at which syslog messages will be sent to the server, thereby providing data samples at even intervals. Enter the desired interval (in minutes). Click **Apply**.

### Rule Usage Auto Clear Ports

This list must contain all ports where you want rule accounting to take place. If you have enabled any of the clear rule usage options, this list must specify the ports on the device where the clear operations will be performed. Click **Add/Remove** to open the [Add Ports window](#) where you can select ports to add to the list. Click **Apply** to set any changes you have made.

## Disabled Ports (Rule / Rate Limit Hit)

This table lists the ports that have been disabled due to rule usage or if a rate limit has been exceeded. For information on how to configure the disabling of a port, refer to the rule [General tab](#) or the rate limit [General tab](#).

### Port

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Retrieve

Retrieves a list of ports on the device that have been disabled due to a rule hit or a rate limit being exceeded.

### Clear

Clears any selected disabled ports, and re-enables them. Keep in mind that if the port continues to receive traffic that matches the rule or exceeds the rate limit, and the rule or rate limit is still configured to disable the port, then the port will almost immediately reappear in the table.

---

## Related Information

For information on related tasks:

- [Rule Accounting and Rule Hit Reporting](#)

For information on related windows:

- [Rule Usage Tab \(Rule\)](#)
- [Rule Usage Tab \(Role/Service/Device\)](#)



## Rule Usage Tab

---

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. This tab displays port information for all the rules that have been used for a selected role, service (manual or automated), device, device group, Policy VLAN Island, Network Resource Topology Island, or for all the devices in the current domain.

To access this tab:

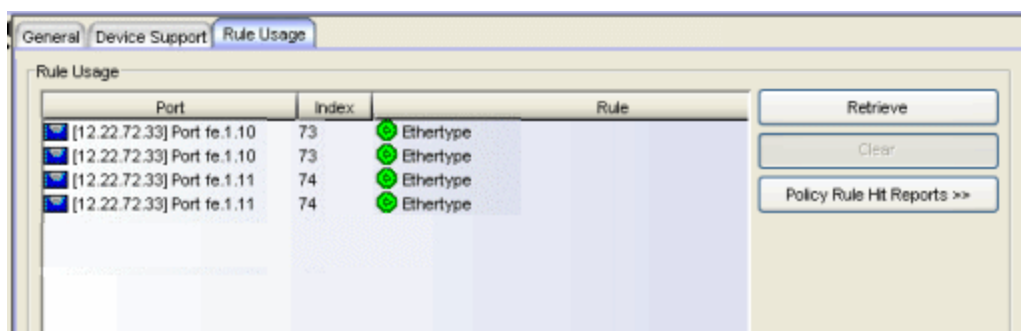
- select a role or service in the left-panel Roles/Services tab
- select a device, device group, or the My Network or All Devices folder in the left-panel Network Elements tab
- select a VLAN island in the left-panel of the Access Control Configuration window (available from the Policy Manager Edit menu)
- select a topology island in the left panel of the Network Resource Configuration window (available from the Policy Manager Edit menu)

then select the Rule Usage tab in the right panel. Click the **Retrieve** button to display the rule usage information. Rule accounting must be enabled on the device; see the [device Role/Rule tab](#) for information.

---

**TIP:** You can see rule accounting information for an individual rule using the [Rule Usage Tab \(Rule\)](#).

---



### Port

Name of the port the rule has been used on.

### Index

The index value assigned to the port interface.

**Rule**

The name of the rule used on the port.

**From Role**

The role that the rule is associated with.

**Retrieve Button**

Retrieves/updates the rule usage information.

**Clear Button**

Clears the selected port(s) from the associated rule's usage list.

**Policy Rule Hit Reports**

Select a port and use this button to access two [Policy Rule Hit Reports](#):

- Policy Rule Hits - this report shows the last 100 rule hits for the selected port.
  - Top-5 Rule Usage Trend (1 week) - this report shows the top five rules with the most rule hits based on the last 7-day period for the selected port.
- 

**Related Information**

For information on related tasks:

- [How to Create or Modify a Rule](#)
- [How to Create a Service](#)

For information on related windows:

- [Role/Rule Tab \(Device\)](#)
- [Rule Usage Tab \(Rule\)](#)

## Rule Usage Tab (Rule)

---

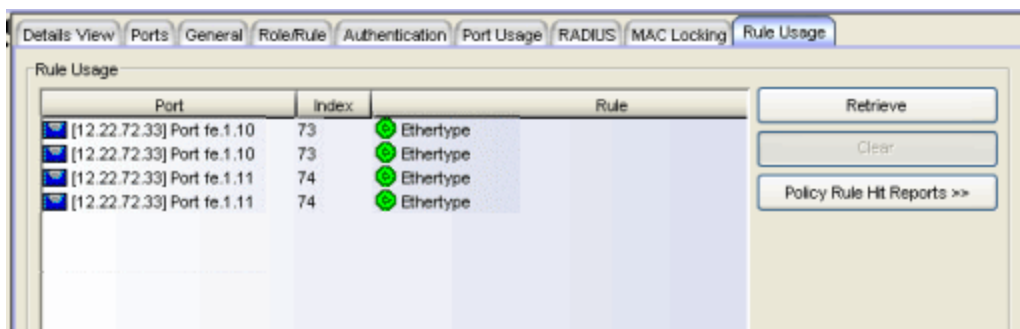
When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. This tab lists the ports on which a selected rule has been used. You can specify options to automatically clear ports from this list in the device [Role/Rule tab](#).

To access this tab, select a rule in the left-panel tree, then select the Rule Usage tab in the right panel. Click the **Retrieve** button to display the rule usage information. Rule accounting must be enabled on the device; see the device [Role/Rule tab](#) for information. If the rule type does not include any devices that support rule accounting, this tab will be grayed out.

---

**TIP:** You can see rule accounting information for all rules associated with a role, service, device, or device group using the [Rule Usage Tab \(Role/Service/Device/Device Group\)](#).

---



### Port

Name of the port the rule has been used on.

### Index

The index value assigned to the port interface.

### Rule

The name of the rule used on the port.

### From Role

The role that the rule is associated with.

### Retrieve Button

Retrieves/updates the rule usage information.

### Clear Button

Clears the selected port(s) from the associated rule's usage list. You can set up auto-clear functionality on a per-port basis in the device [Role/Rule tab](#).

### Policy Rule Hit Reports

Select a port and use this button to access two [Policy Rule Hit Reports](#):

- Policy Rule Hits - this report shows the last 100 rule hits for the selected port.
- Top-5 Rule Usage Trend (1 week) - this report shows the top five rules with the most rule hits based on the last 7-day period for the selected port.

---

### Related Information

For information on related tasks:

- [How to Create or Modify a Rule](#)
- [How to Configure Devices](#)

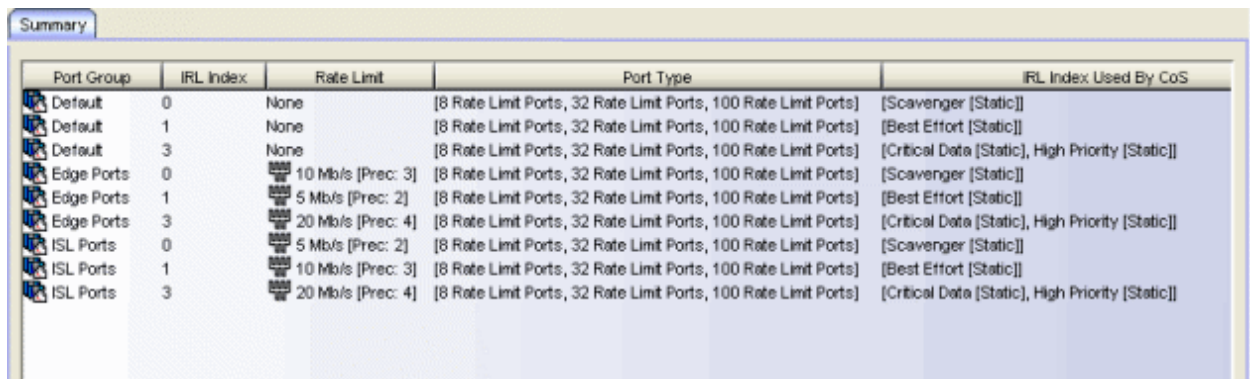
For information on related windows:

- [Role/Rule Tab \(Device\)](#)
- [Rule Usage Tab \(Role/Service/Device/Device Group\)](#)

## Summary Tab (Rate Limit Port Groups Folder)

This tab lists all the inbound or outbound rate limit port groups, along with their rate limit mapping information. Rate limit mappings map a logical rate limit index (IRL/ORL Index) to an actual physical rate limit. You can configure a port group's mappings on the port group [Mappings tab](#).

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a rate limit port group folder in the tree, and the Summary tab will be displayed in the right panel.



Port Group	IRL Index	Rate Limit	Port Type	IRL Index Used By CoS
Default	0	None	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Scavenger [Static]]
Default	1	None	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Best Effort [Static]]
Default	3	None	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Critical Data [Static], High Priority [Static]]
Edge Ports	0	10 Mb/s [Prec: 3]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Scavenger [Static]]
Edge Ports	1	5 Mb/s [Prec: 2]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Best Effort [Static]]
Edge Ports	3	20 Mb/s [Prec: 4]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Critical Data [Static], High Priority [Static]]
ISL Ports	0	5 Mb/s [Prec: 2]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Scavenger [Static]]
ISL Ports	1	10 Mb/s [Prec: 3]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Best Effort [Static]]
ISL Ports	3	20 Mb/s [Prec: 4]	[8 Rate Limit Ports, 32 Rate Limit Ports, 100 Rate Limit Ports]	[Critical Data [Static], High Priority [Static]]

### Port Group

The name of the port group.

### IRL/ORL Index

The logical rate limit index number.

### Rate Limit

The actual rate limit that the index is mapped to.

### Port Type

The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).

### IRL/ORL Index Used By CoS

The Class of Service using this index.

## **Related Information**

For information on related concepts:

- [Getting Started with Class of Service](#)

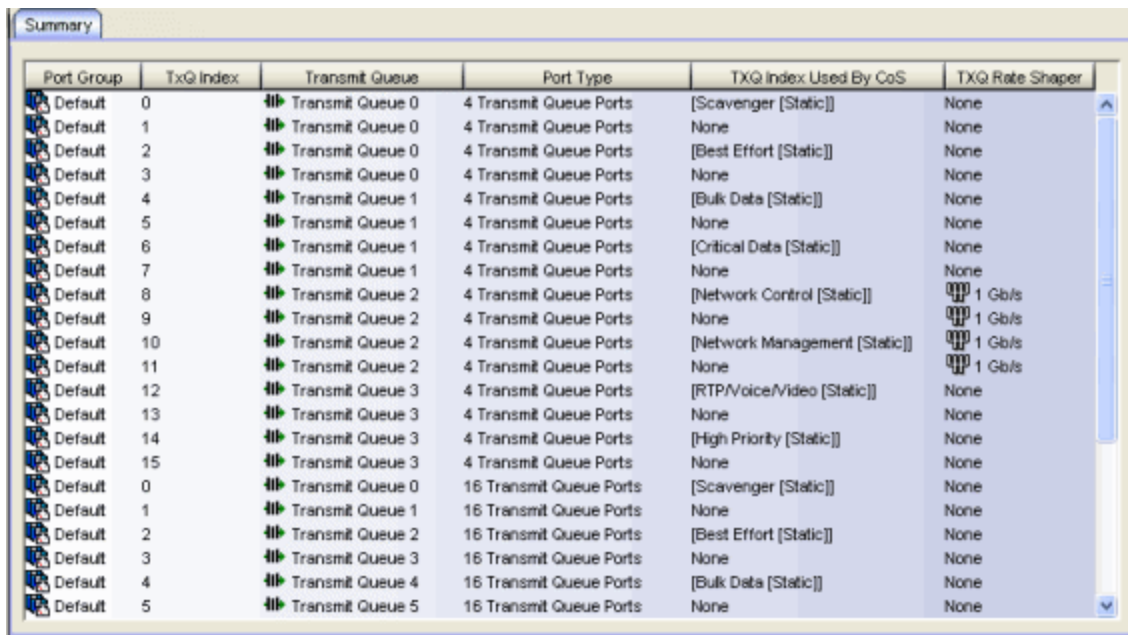
For information on related tasks:

- [Creating Class of Service Port Groups](#)

## Summary Tab (Transmit Queue Port Groups Folder)

This tab displays transmit queue mapping information for one or more port groups, depending on what you have selected in the left panel of the Class of Service Configuration window. Transmit queue mapping maps a logical transmit queue index (used by a class of service) to an actual physical transmit queue you have configured in Policy Manager. You can configure transmit queue mappings for a port group using the [CoS - Transmit Queue Mappings tab](#).

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select a transmit queue port group folder in the tree, and the Summary tab will be displayed in the right panel.



Port Group	TxQ Index	Transmit Queue	Port Type	TXQ Index Used By CoS	TXQ Rate Shaper
Default	0	Transmit Queue 0	4 Transmit Queue Ports	[Scavenger [Static]]	None
Default	1	Transmit Queue 0	4 Transmit Queue Ports	None	None
Default	2	Transmit Queue 0	4 Transmit Queue Ports	[Best Effort [Static]]	None
Default	3	Transmit Queue 0	4 Transmit Queue Ports	None	None
Default	4	Transmit Queue 1	4 Transmit Queue Ports	[Bulk Data [Static]]	None
Default	5	Transmit Queue 1	4 Transmit Queue Ports	None	None
Default	6	Transmit Queue 1	4 Transmit Queue Ports	[Critical Data [Static]]	None
Default	7	Transmit Queue 1	4 Transmit Queue Ports	None	None
Default	8	Transmit Queue 2	4 Transmit Queue Ports	[Network Control [Static]]	1 Gb/s
Default	9	Transmit Queue 2	4 Transmit Queue Ports	None	1 Gb/s
Default	10	Transmit Queue 2	4 Transmit Queue Ports	[Network Management [Static]]	1 Gb/s
Default	11	Transmit Queue 2	4 Transmit Queue Ports	None	1 Gb/s
Default	12	Transmit Queue 3	4 Transmit Queue Ports	[RTP/Voice/Video [Static]]	None
Default	13	Transmit Queue 3	4 Transmit Queue Ports	None	None
Default	14	Transmit Queue 3	4 Transmit Queue Ports	[High Priority [Static]]	None
Default	15	Transmit Queue 3	4 Transmit Queue Ports	None	None
Default	0	Transmit Queue 0	16 Transmit Queue Ports	[Scavenger [Static]]	None
Default	1	Transmit Queue 1	16 Transmit Queue Ports	None	None
Default	2	Transmit Queue 2	16 Transmit Queue Ports	[Best Effort [Static]]	None
Default	3	Transmit Queue 3	16 Transmit Queue Ports	None	None
Default	4	Transmit Queue 4	16 Transmit Queue Ports	[Bulk Data [Static]]	None
Default	5	Transmit Queue 5	16 Transmit Queue Ports	None	None

### Port Group

The name of the transmit queue port group.

### TXQ Index

The logical transmit queue index.

### Transmit Queue

The physical transmit queue that the transmit queue index is mapped to.

### Port Type

Port type is based on the number of transmit queues the port supports.

### TXQ Index Used By CoS

The Class of Service using this TXQ index.

### TXQ Rate Shaper

The transmit queue's associated rate shaper as configured in the transmit queue's General tab.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

For information on related windows:

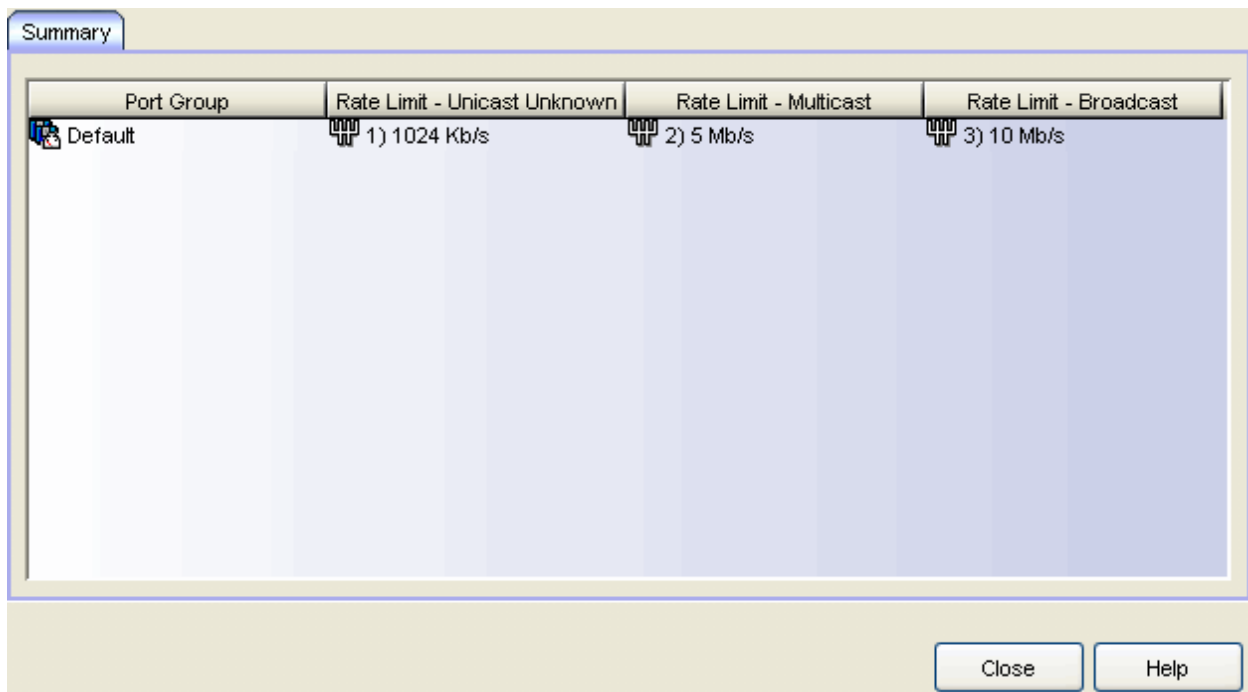
- [CoS - Transmit Queue Mappings Tab \(Transmit Queue Port Group\)](#)
- [Arbiter Mode Tab \(Transmit Queue Port Group\)](#)
- [Ports Tab \(Transmit Queue Port Group\)](#)



## Summary Tab (Flood Control Port Groups)

This tab lists the flood control rates per port group. Each port group supports rate limits for three separate configured traffic types (Unicast, Multicast, and Broadcast). As flood control is enabled/disabled for a Class of Service, when enabled, each column will either display a rate limit, or "No Rate" if no rate has been defined for that portion of flood control.

To access this tab, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, select the "Show all CoS Components in Tree (Advanced Mode)" option from the Domain Managed CoS Components menu to display the CoS tree in the left panel. Select the Flood Control Port Groups folder in the tree, and the Summary tab will be displayed in the right panel.



Port Group	Rate Limit - Unicast Unknown	Rate Limit - Multicast	Rate Limit - Broadcast
Default	1) 1024 Kb/s	2) 5 Mb/s	3) 10 Mb/s

### Port Group

The name of the port group.

### Rate Limit - Unicast

The configured traffic flood control rate limit for Unicast traffic.

### Rate Limit - Multicast

The configured traffic flood control rate limit for Multicast traffic.

### Rate Limit - Broadcast

The configured traffic flood control rate limit for Broadcast traffic.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Configure Flood Control](#)

For information on related windows:

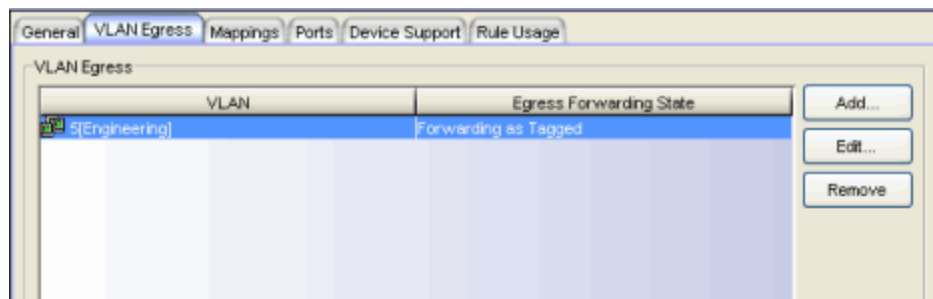
- [General Tab \(Rate Limit\)](#)

## VLAN Egress Tab (Role)

---

The role VLAN Egress tab displays the list of VLANs on the selected role's egress list, and allows you to add and remove VLANs and set their Egress Forwarding State. Ports that the selected role is active on will forward traffic belonging to the listed VLANs according to the specified forwarding state. Both the role's egress list and the VLAN egress list are checked for egress information. If the lists have duplications, the Forbid Forwarding state takes precedence.

To access this tab, select a role in the left panel's Roles tab and click the VLAN Egress tab in the right panel. Any changes made on this tab need to be enforced with the **Enforce** button on the toolbar.



### VLAN

The VLAN ID and name.

### Egress Forwarding State

Ports the selected role is active on will forward traffic belonging to this VLAN according to the egress forwarding state: Tagged (frames will be forwarded as tagged), Untagged (frames will be forwarded as untagged), or Forbid Forwarding (frames will not be forwarded; they will be discarded).

### Add

Opens the Egress VLANs [Selection View](#), where you can choose a VLAN for the role's egress list and specify the egress forwarding state.

### Edit

Select a VLAN in the table and click **Edit** to open the Egress VLANs [Selection View](#), where you can change the VLAN's egress forwarding state. You can also double-click a VLAN in the table to edit the VLAN.

### Remove

Select a VLAN and click **Remove** to remove the VLAN from the list.

### **Related Information**

For information on related windows:

- [Selection View \(Egress VLANs\)](#)

## VLANs Tab (Policy VLAN Islands)

---

This tab displays a table of the Island VLANs being used in the [Policy VLAN Island](#), and the names created on the devices in the island. To display this tab, select the VLAN island in the left panel of the Access Control Configuration window (available from the Policy Manager Edit menu), and the VLANs tab in the right panel.

The **VLANs Tab** provides two sub-tabs:

- [\(VLAN\) - VIDs Tab](#)
- [\(VLAN\) - Role Mappings Tab](#)

### (VLAN) - VIDs Tab

This tab provides information on islands assigned to specific VLANs. When a VLAN is selected, the tabs in the VLAN Settings section update to reflect the data for that VLAN including the Island Name and the Island VLAN ID assigned to each defined island.

Policy VLAN Islands (PVI) allow Roles and Rules using VLAN containment Access Control to vary the VID across the network based on the Island where a user connects to the network. This can allow the network to isolate resources, for instance putting traffic from visitors in a "Guest" PVI VLAN that uses a different VID for each campus of a company.

Below, select a PVI VLAN to see the specific VLANs used for that VLAN in each island as well as the Role mappings assigned to that VLAN.

**VLANs**

- Guest
- Restricted

**VLAN Settings**

Restricted - VLANs

Island Name	Island VLAN ID
Default Island	None
North Campus	None
South Campus	None

Buttons: Edit Island VLAN ID, Show all VLANs for Island

Buttons: Close, Help

## VLANs

List of created VLANs.

## Island Name

Name of the island VLAN that is being used to create VLANs in the VLAN island.

## Island VLAN ID

VLAN ID assigned to the device in the VLAN island.

## Edit Island VLAN ID

Selecting a VLAN in the table and clicking this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

---

**NOTE:** If the VLAN IDs are recalculated (for example, if you change the base or offset for the VLAN island), any changes you made to island VLAN IDs will be lost.

---

**Show all VLANs for Island**

Selecting an island in the table and clicking this button opens the selected VLAN island's [VLANs tab](#).

**Create**

Opens the Create VLAN dialog. For more information, see [Creating a VLAN Island](#).

## (VLAN) - Role Mappings Tab

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see [VLAN to Role Mapping](#) in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

**VLANs**

List of created VLANs.

**Tagged Packet VLAN to Role Mapping**

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingress with.

**Port Level Mappings**

This table lists any port-level Tagged Packet VLAN to Role Mappings that have been configured for this VLAN. Port-level mappings will override any device-level mapping.

**Create**

Opens the Create VLAN dialog. For more information, see [Creating a VLAN Island](#).

---

**Related Information**

For information on related concepts:

- [Policy VLAN Islands](#)
- [VLAN to Role mapping](#)

For information on related tasks:

- [How to Create a Policy VLAN Island](#)



# Policy Manager Windows

---

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

## Add/Edit CEP Detection Rule Window

Use this window to add or edit CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected. Access the window from the CEP Detection sub-tab in the right-panel [Device Authentication tab](#).

**NOTE:** CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection - Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones will be detected on TCP/UDP port 4060.
- IP Address detection - H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules that will detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones will be detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones will be detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones will also be detected using only their respective multicast addresses without the TCP/UDP ports.

The screenshot shows the 'Add CEP Detection Entry' dialog box. The 'CEP Detection Settings' section includes the following fields and values:

Field	Value
Priority	1
Address	224.0.1.41
Address Mask	
End Point Type	h323
Protocol	<input checked="" type="checkbox"/> UDP <input checked="" type="checkbox"/> TCP
Low Port	1718
High Port	1720

Buttons on the right: OK, Apply, Cancel, Help.

## CEP Detection Settings

### Priority

Enter the rule priority with one (1) being the highest priority. The rule with the highest priority will be used first, so it is recommended that the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

### Address

If the rule is based on IP address detection, enter the IP address that incoming packets will be matched against. By default, H.323 will use 224.0.1.41 as its IP address, SIP will use 224.0.1.75 as its IP address, and Siemens will have no IP address configured.

### Address Mask

If the rule is based on IP address detection, enter the IP address mask that incoming packets will be matched against.

### End Point Type

Select the endpoint type (H.323, Siemens, or SIP) that will be assigned if incoming packets match this rule.

### Protocol

If the rule is based on TCP/UDP port detection, select the UDP and/or TCP checkbox and define a port range with Port Low and Port High values:

- UDP and TCP - Match the port number for both UDP and TCP frames.
- TCP - Match the port number only for TCP frames.
- UDP - Match the port number only for UDP frames.

### Port Low

Define the low end of the port range for detection on UDP and/or TCP ports.

### Port High

Define the high end of the port range for detection on UDP and/or TCP ports.

---

## Related Information

For information on related windows:

- [Device Authentication Tab](#)

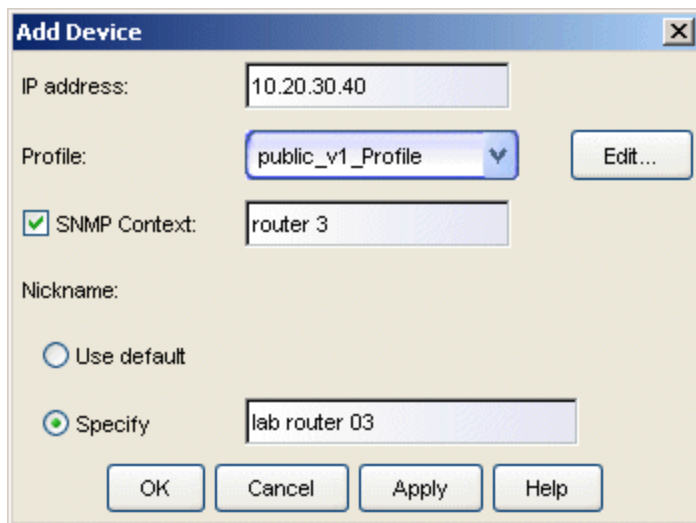
For information on related tasks:

- [How to Configure Devices](#)
- [How to Configure CEP](#)

## Add Device Window

---

This window lets you add a single device to your NetSight database, as opposed to [discovering](#) devices or [importing](#) devices from a device list. When you add a device, it is assigned to the current domain and automatically listed in the left-panel device tree. You can access this window by right-clicking a group in the left-panel Network Elements tab and choosing **Add Device** from the right-click menu.



### IP Address

Enter the IP address of the device you want to add.

### Profile

Use the 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.

### SNMP Context

Select the checkbox and enter an SNMP context that has been configured on the device. An SNMP context is a collection of MIB objects, often associated with an entity. By specifying the SNMP context here, you can access the subset of MIB objects related to that context on the device.

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. Then, when SNMPv1/v2 credentials are used, access is granted to the subset of MIB objects associated with that credential (community name).

Policy Manager treats each context for a given device (IP address) as a distinct device. The devices are displayed in the tree with the same IP address followed by the different SNMP contexts. 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.

### 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.

---

### Related Information

For information on related tasks:

- [How to Add and Delete Devices](#)

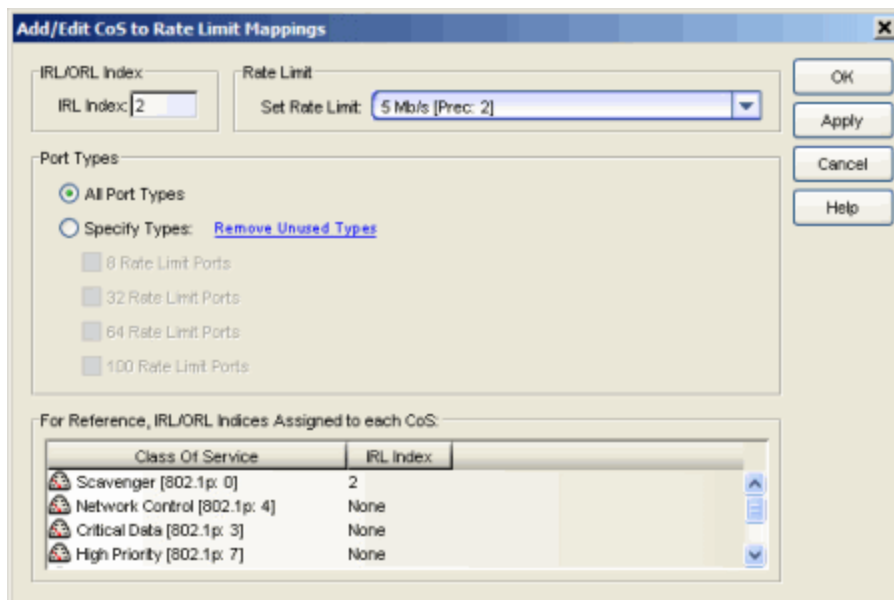
## Add/Edit CoS to Rate Limit Mappings Window

---

This window lets you configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index to an actual physical rate limit you have created in Policy Manager.

For reference, the CoS IRL/ORL Index table (at the bottom of the window) displays classes of service that already have an IRL/ORL index specified, so that you can see which classes of service will be affected by mapping an index to a rate limit.

To access this window, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Click on the **Domain Managed CoS Components** button and select the **Show all CoS Components in Tree (Advanced Mode)** menu option. Select a rate limit port group in the left-panel Classes of Service tab. Then, select the [CoS - Rate Limit Mappings tab](#) in the right panel and click the **Add/Edit** button.



### IRL/ORL Index

Specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.

---

**TIP:** Use the **Apply** button to map all your indexes without having to close and re-open the window.

---

### Rate Limit

Use the drop-down list to select a rate limit to map to the index. Rate limits are listed by the rate limit name followed by the precedence. Select "Create" to open the [Create Rate Limit/Shaper Window](#) where you can define a new rate limit. For information on how to create a rate limit, see [How to Define Rate Limits](#). Select "None" to remove an existing mapping for the specified port types.

### Port Types

These options allow you to create a mapping for all port types at once, or create a mapping just for specific port types.

### CoS IRL/ORL Index Usage

This table displays the IRL or ORL indexes being used by each class of service (CoS). You can use this table to determine which classes of service will use the rate limit, depending on whether the class of service has been mapped to an IRL/ORL. For example, in the screenshot above, you can see that if you map the IRL Index 2 to the 5 Mb/s rate, then the Scavenger CoS will use this rate for all ports in this port group.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [Defining Rate Limits](#)
- [Advanced Rate Limiting by Port Type](#)

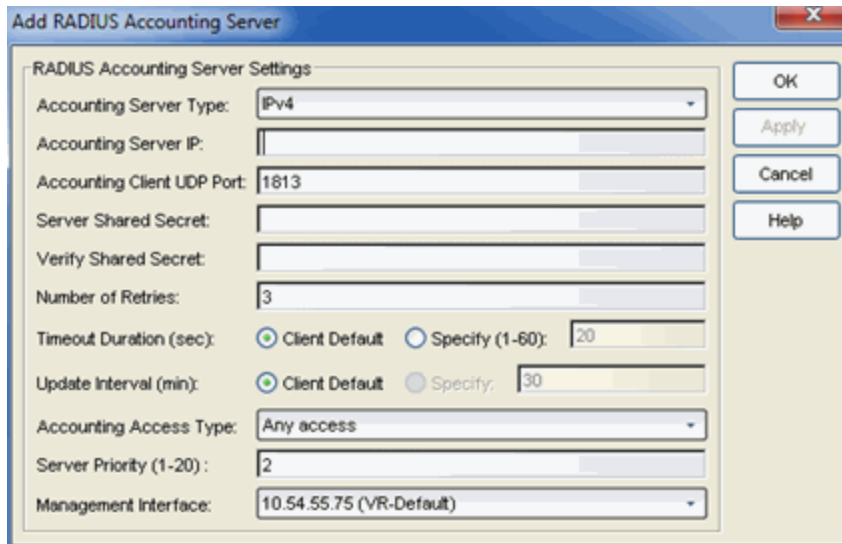
For information on related windows:

- [Ports Tab \(Rate Limit Port Group\)](#)



## Add RADIUS Accounting Server Window

This window lets you add a RADIUS server to Policy Manager for the purpose of RADIUS accounting. Access this window by clicking **Add** in the RADIUS Server (s) Accounting sub-tab in the [RADIUS tab](#) for a device.



### Accounting Server Type

Select the accounting type used on the RADIUS server.

**NOTE:** DNS is only available as an option if there is a valid DNS server configured on the device so the DNS name can resolve to an IP address when configuration occurs.

### Accounting Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS accounting server. Not all devices support IPv6 address types.

### Accounting Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send accounting requests to the RADIUS server; 1813 is the default port number. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS accounting server.

This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

**NOTE:** This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and Policy Manager, entered in the Application Shared Secret area of the [RADIUS tab](#) for a device.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

### Number of Retries (0-20)

The number of times the device will resend an accounting request if the RADIUS server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Timeout Duration (2 -10 sec)

The amount of time in seconds the device will wait for the RADIUS server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Update Interval (minutes)

The Accounting Update Interval is the amount of time in minutes between accounting updates. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Accounting Client Settings](#) section of the RADIUS tab. Devices that do not support RADIUS accounting will have this field grayed out.

### Accounting Access Type

Use the drop-down menu to select the type of accounting access allowed for this RADIUS server:

- **Any access** - the server can send an accounting request for users originating from any access type.
- **Management access** - the server can only send an accounting request for users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only send an accounting request users that are accessing the network via 802.1X, MAC, or Web-Based accounting.

This feature allows you to have one set of servers for accounting management access requests and a different set for accounting network access requests. Devices that do not support this feature have this field grayed out.

#### Server Priority (1-20)

Order in which the RADIUS accounting server will be checked, as compared to the other RADIUS accounting servers on the device. The lower the number, the higher the priority.

#### Management Interface

Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

**NOTE:** ExtremeXOS devices must define a Management Interface.

---

#### Related Information

For information on related windows:

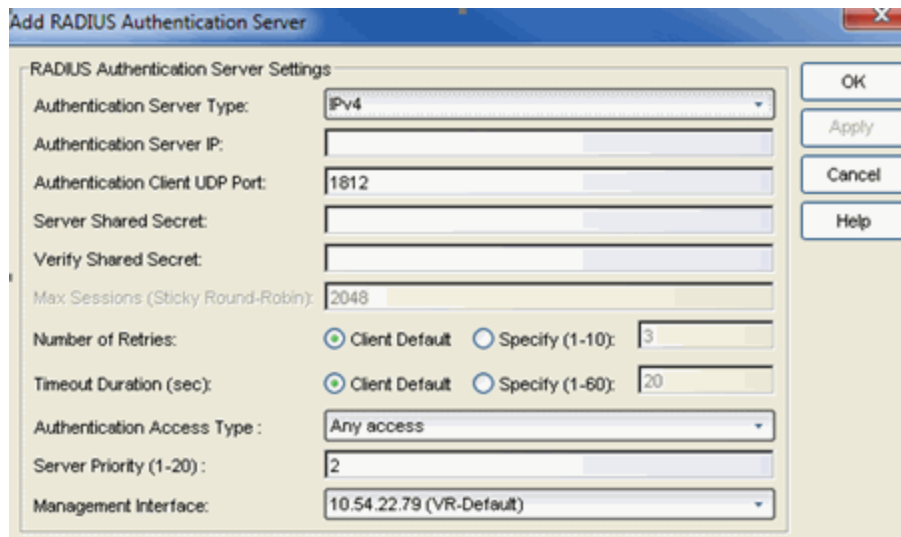
- [RADIUS Tab](#)

For information on related tasks:

- [How to Configure Devices](#)

## Add RADIUS Authentication Server Window

This window lets you add a RADIUS server to Policy Manager for the purpose of authentication. Access this window by clicking **Add** in the RADIUS Server(s) Authentication sub-tab in the [RADIUS tab](#) for a device.



### Authentication Server Type

Select the authentication type used on the RADIUS server.

**NOTE:** DNS is only available as an option if there is a valid DNS server configured on the device so the DNS name can resolve to an IP address when configuration occurs.

### Authentication Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS authentication server. Not all devices support IPv6 address types.

### Authentication Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send authentication requests to the RADIUS authentication server; 1812 is the default port number.

### Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS authentication server. This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate, and authentication attempts will

fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

**NOTE:** This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and Policy Manager, entered in the Application Shared Secret area of the [RADIUS tab](#) for a device.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

### Max Sessions (Sticky Round-Robin)

Specifies the maximum number of sticky round-robin authentication sessions allowed on the server when the [sticky round-robin RADIUS authentication algorithm](#) is configured for a device. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to. Devices that do not support this functionality will have the option grayed out.

### Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless Wireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section of the RADIUS tab.

### Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless Wireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section of the RADIUS tab.

### Authentication Access Type

Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- **Any access** - the server can authenticate users originating from any access type.
- **Management access** - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

This feature allows you to have one set of servers for authenticating management access requests and a different set for authenticating network access requests. Devices that do not support this feature will have this field grayed out.

### Server Priority

Order in which the RADIUS authentication server will be checked, as compared to the other RADIUS authentication servers on the device. The lower the number, the higher the priority.

### Management Interface

Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

**NOTE:** ExtremeXOS devices must define a Management Interface.

---

### Related Information

For information on related concepts:

- [Authentication](#)

For information on related windows:

- [RADIUS Tab](#)

For information on related tasks:

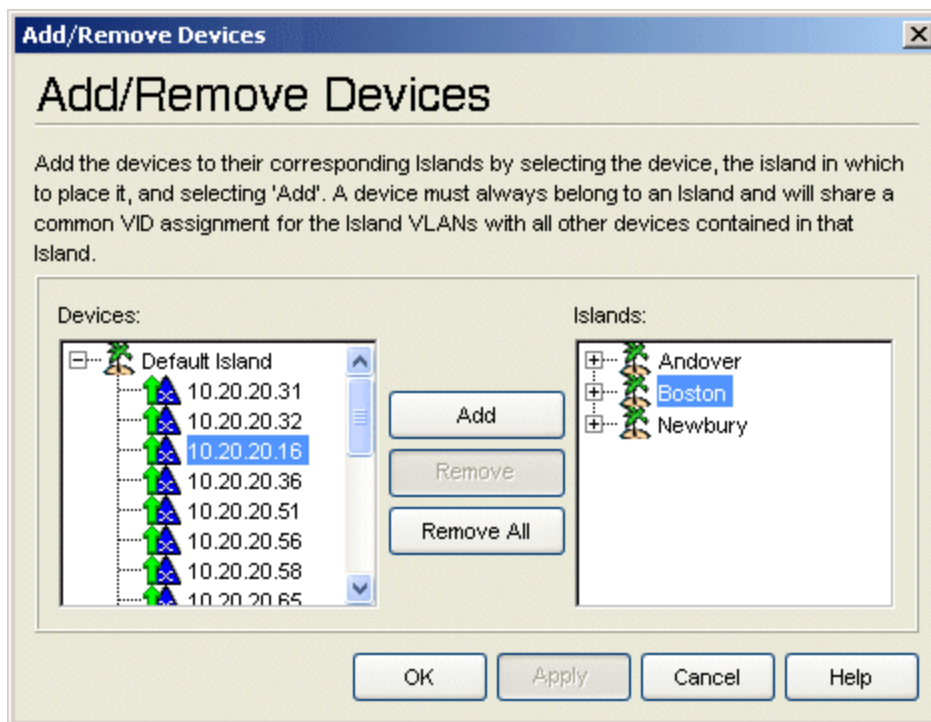
- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)

## Add/Remove Devices Window (VLAN Islands)

This window enables you to add and remove devices from VLAN islands. To access the window, right-click a VLAN island in the left-panel VLANs tab and select **Add/Remove Devices** from the menu.

Devices contained in an island will be assigned a VID for each Island VLAN that is unique to the island, allowing roles and rules which use the Island VLANs to isolate users to that island. A device must always belong to an island, and will share a common VID assignment for the Island VLANs with all other devices contained in that island.

To add a device to an island, select the device in the left panel and either drag it to the island, or select the island and click **Add**. You can also select and add multiple devices.



### Devices

Expand the Default Island folder to select the device or devices to add.

### Islands

This panel displays all the user-defined VLAN islands and the devices that are members of the islands. Select a device and click **Remove** to remove the

device from the island.

### **Add Button**

Adds the device(s) selected in the Devices panel to the island selected in the Islands panel. You can also add a device using drag and drop.

### **Remove Button**

Removes the device(s) selected in the Islands panel from the VLAN island.

### **Remove All Button**

Removes all the devices from the VLAN island selected in the Islands panel.

---

## **Related Information**

For information on related concepts:

- [Policy VLAN Islands](#)


For information on related tasks:

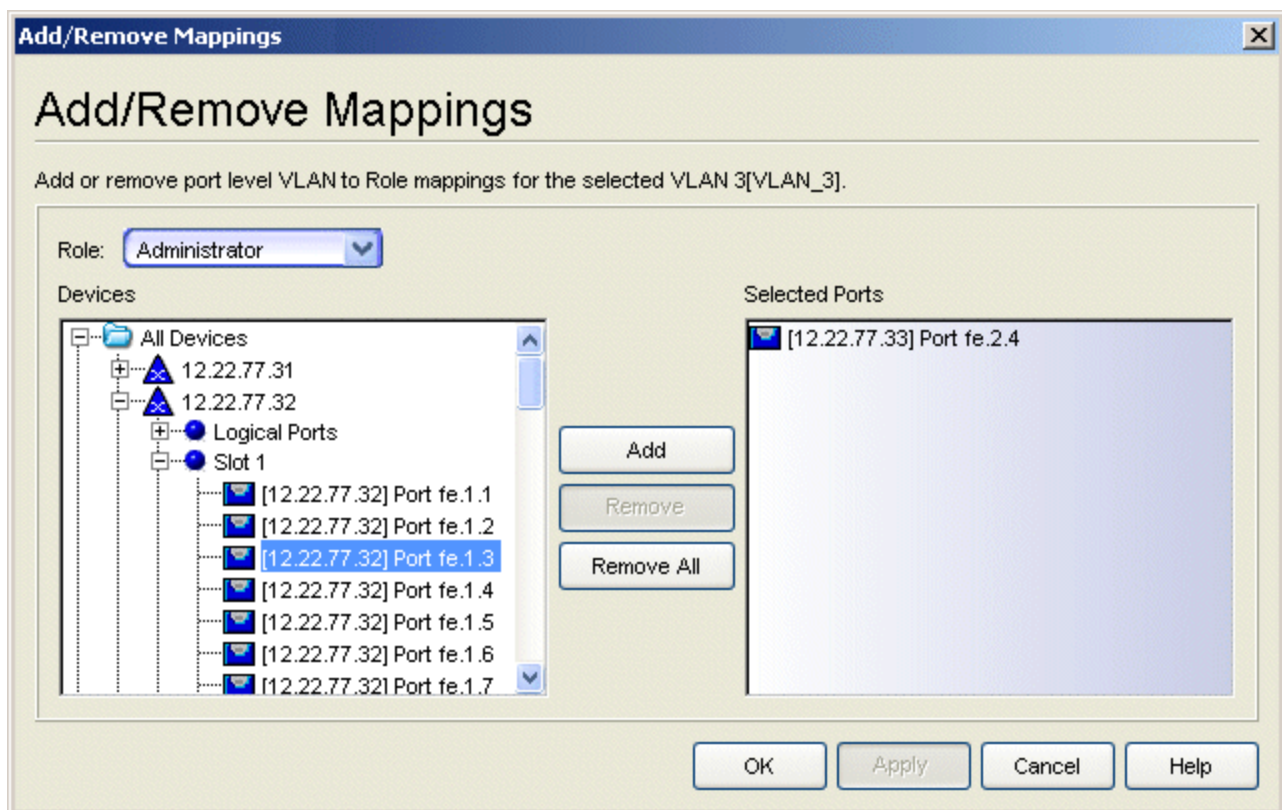
- [How to Create a Policy VLAN Island](#)



## Add/Remove Mappings Window (Port-Level Mappings)

In the Add/Remove Mappings window, you can add or remove port-level Tagged Packet VLAN to Role mappings for a selected VLAN. To access this window, first select a VLAN in the left panel of the Access Control Configuration window (available from the Policy Manager Edit menu). Then, in the right-panel [General tab](#), select the **Add/Remove Mappings** button in the Port Level Mappings section.

**NOTE:** You cannot add or remove a port-level mapping to or from a frozen port . You must clear the frozen state on a port in order to add or remove a mapping.



### Role

Use the drop-down list to select the role being mapped.

### Devices

This field displays all the device groups, devices, and port groups in the current domain. If you are adding a mapping to a port, select the desired port or ports. You can select an individual port, one or more devices, or groups of ports.

### Selected Ports

This field displays all the ports currently defined for the mapping. You can remove one or more ports from the list by selecting the port and clicking **Remove** or you can remove all the ports by clicking **Remove All**.

### Add Button

Adds the ports selected in the Devices field to the Selected Ports field. You can also add ports by double clicking or using drag and drop.

### Remove Button

Removes the ports selected in the Selected Ports field. You can also double click a port to remove it.

### Remove All Button

Removes all the ports in the Selected Ports field.

---

## Related Information

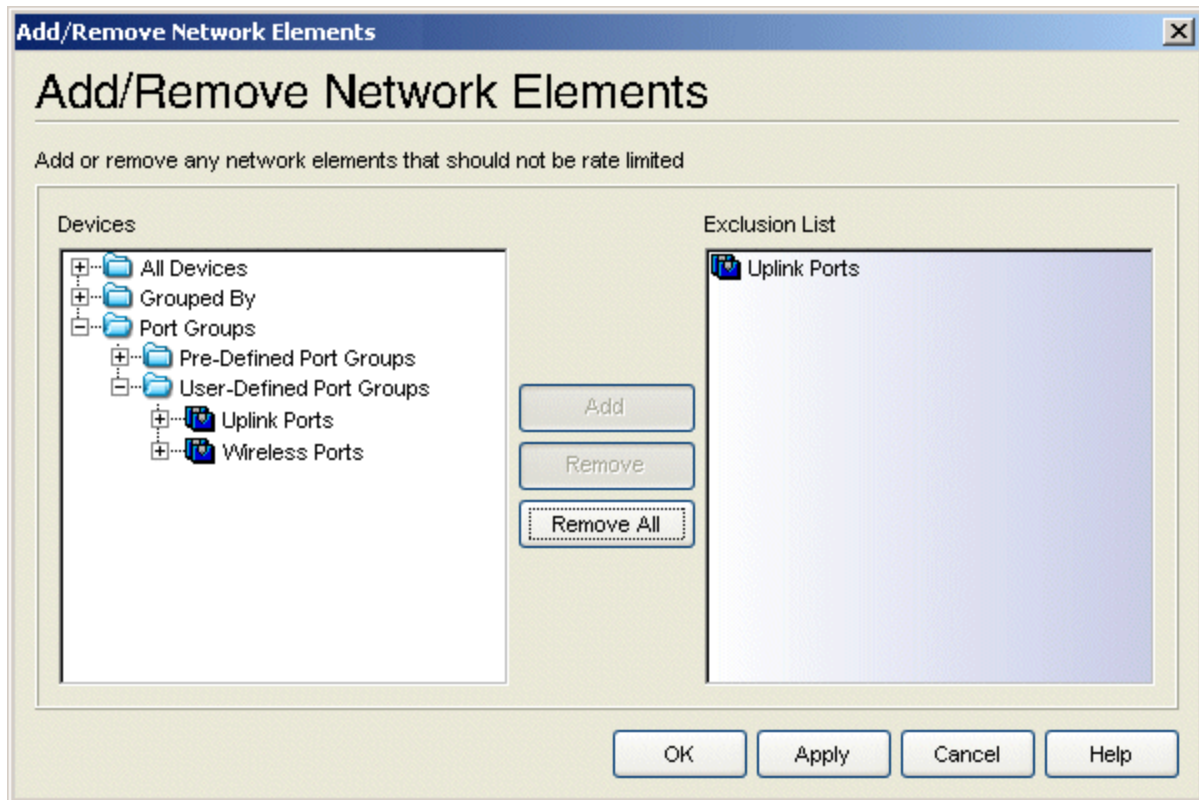
For information on related windows:

- [General Tab \(VLAN\)](#)
- [Mappings Tab \(Role\)](#)
- [Port Properties Window - General Tab](#)

## Add/Remove Network Elements Window

You can exclude specified network elements from the effects of a rate limit using the Add/Remove Network Elements window.

To access this window, select the rate limit in the left-panel Classes of Service tab and make sure the General tab is displayed in the right panel. In the Exclusion section of the General tab, click **Edit**



### Devices

This list displays all the network elements in the current domain. [Select](#) any network elements you do not want to be affected by the rate limit.

### Exclusion List

This list displays the network elements currently excluded from the rate limit. [Select](#) any network elements you want to remove from this list. Removing a network element from the Exclusion List means it can then be affected by the rate limit.

### **Add Button**

Adds the network elements selected in the Devices list to the Exclusion List. You can also add a network element to the Exclusion List by using drag and drop.

### **Remove Button**

Removes the network elements selected in the Exclusion List. You can also double click a network element to remove it.

### **Remove All Button**

Removes all the network elements from the Exclusion List.

---

## **Related Information**

For information on related tasks:

- [How to Define a Rate Limit](#)

For information on related windows:

- [General Tab \(Rate Limit\)](#)

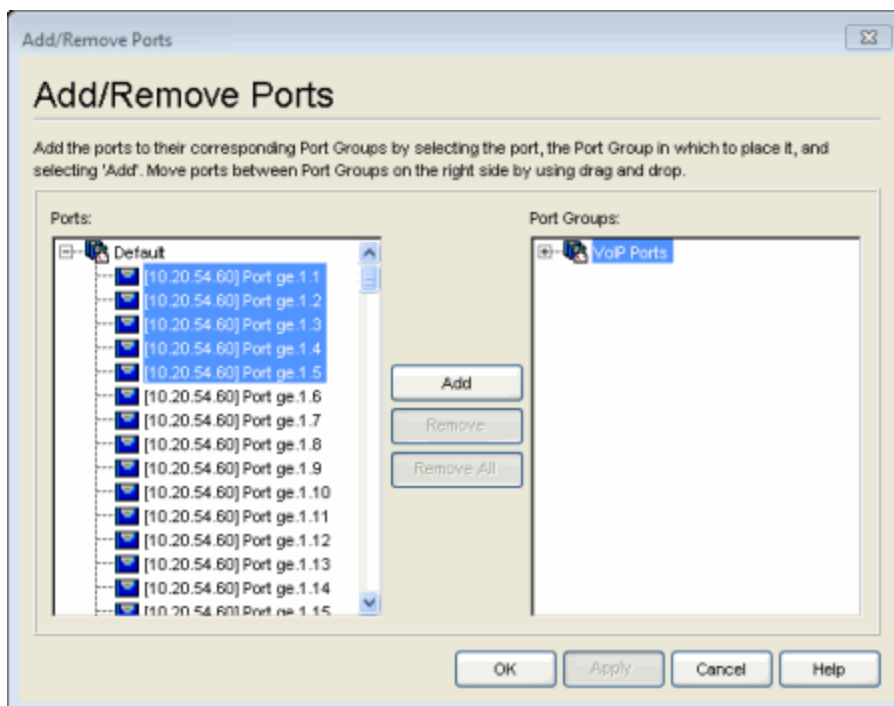
## Add/Remove Ports Window (Rate Limit and Transmit Queue Port Groups)

In this window, you can add and remove ports to and from rate limit port groups and transmit queue port groups. Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups using this window.

To access this window, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Then, right-click on a port group column heading and select Add/Remove Ports. The Add/Remove Ports window opens with the ports in the Default port group displayed in the left panel.

Add ports to the port group by selecting the ports in the left-panel, then selecting the port group in the right panel and clicking **Add**. You can also move ports between port groups in the right panel using drag and drop.

**Note:** User based ports are not listed because user based port groups can only be one default.



### Ports

This field displays the Default port group. Initially, all ports are grouped into the Default port group.

### Port Groups

This field displays any rate limit or transmit queue port groups you have created and their currently defined ports.

### Add Button

Adds the ports selected under the Default port group to the port group selected on the right. You can also add ports to a group using drag and drop.

### Remove Button

Select the ports you want to remove from a port group and click **Remove** to return the ports to the Default port group.

### Remove All Button

Select a port group and click **Remove All** to remove all ports from the port group and return them to the Default port group.

---

## Related Information

For information on related concepts:

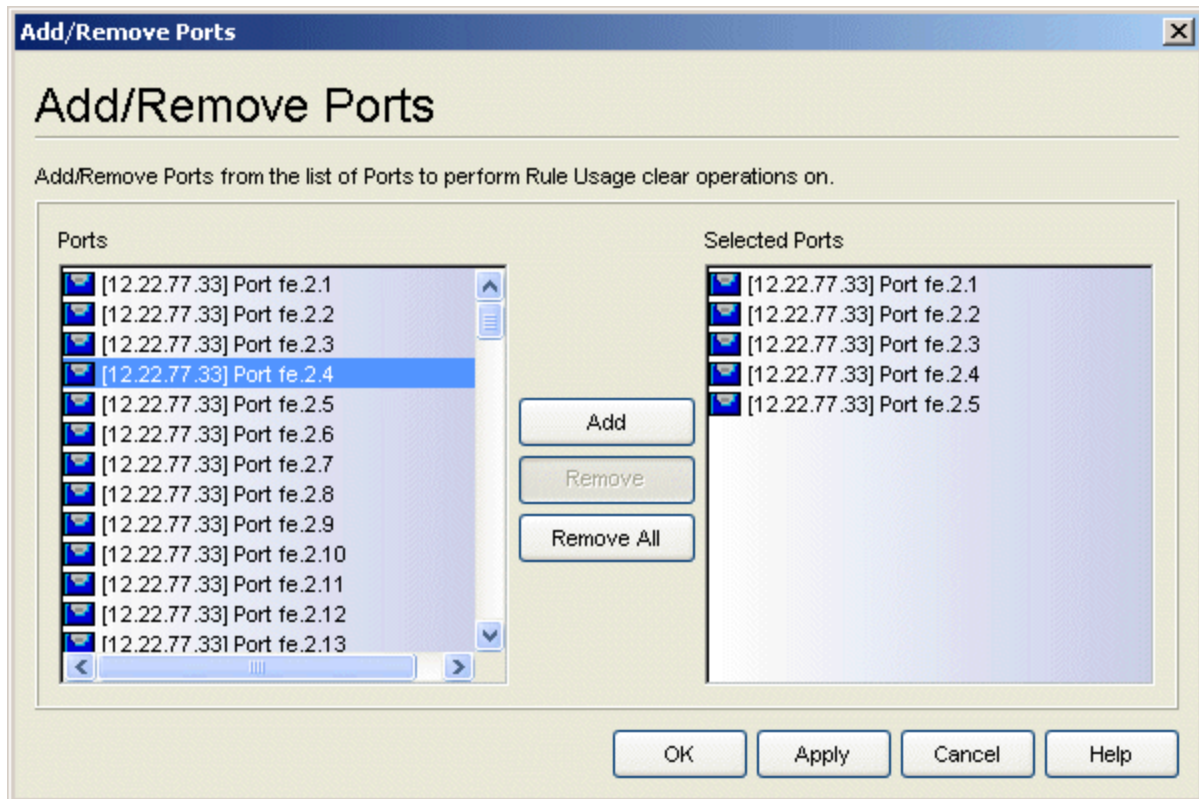
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Define Rate Limits](#)
- [Creating Class of Service Port Groups](#)
- [How to Configure Transmit Queues](#)

## Add/Remove Ports Window (Rule Usage Auto Clear)

Use this window to add or remove ports to and from the Rule Usage Auto Clear Ports list in the device [Role/Rule tab](#).



### Ports

Lists all the ports on the device. [Select](#) the ports you want to add to the list and click **Add**.

### Selected Ports

Lists all the ports currently selected for the list. [Select](#) any ports you want to remove from the list and click **Remove**.

### Add Button

Click **Add** to add the ports selected in the Ports list. You can also add ports by double clicking or using drag and drop.

### Remove Button

Click **Remove** to remove the ports selected in the Selected Ports list. You can also double click a port to remove it.

### Remove All Button

Click **Remove All** to remove all the ports in the Selected Ports list.

---

### Related Information

For information on related windows:

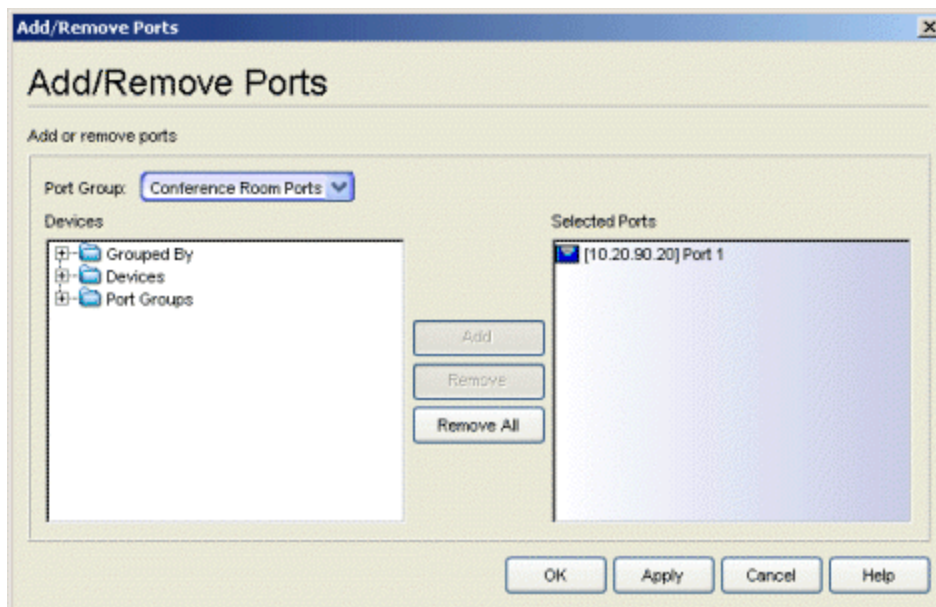
- [Role/Rule Tab \(Device\)](#)



## Add/Remove Ports Window (User-Defined Port Groups)

Use the Add/Remove Ports window to add and remove ports from user-defined port groups. To access this window, select the left-panel Port Groups tab. Expand the User-Defined Port Groups folder and select a port group. Then, you can either:

- Right-click the port group and select **Add/Remove Ports** from the menu, or
- Click the **Add/Remove Ports** button in the right-panel Ports tab.



### Port Group

Use the drop-down list to select the port group where you want to add or remove ports.

### Devices

This field displays all the device groups, devices, and port groups in the current domain. [Select](#) the ports you want to add to the port group. You can select individual ports, devices, or groups of ports.

### Selected Ports

This field displays all the ports currently defined for the port group. [Select](#) the port you want to remove from the port group.

### Add Button

Click **Add** to add the ports selected in the Devices field to the Selected Ports field. You can also add ports by double clicking or using drag and drop.

### Remove Button

Click **Remove** to remove the ports selected in the Selected Ports field from the port group. You can also double click a port to remove it.

### Remove All Button

Click **Remove All** to remove all the ports in the Selected Ports field.

---

## Related Information

For information on related tasks:

- [Adding Ports to a Port Group](#)
- [Removing Ports from a Port Group](#)

## Add/Remove Services Window (Roles)

---

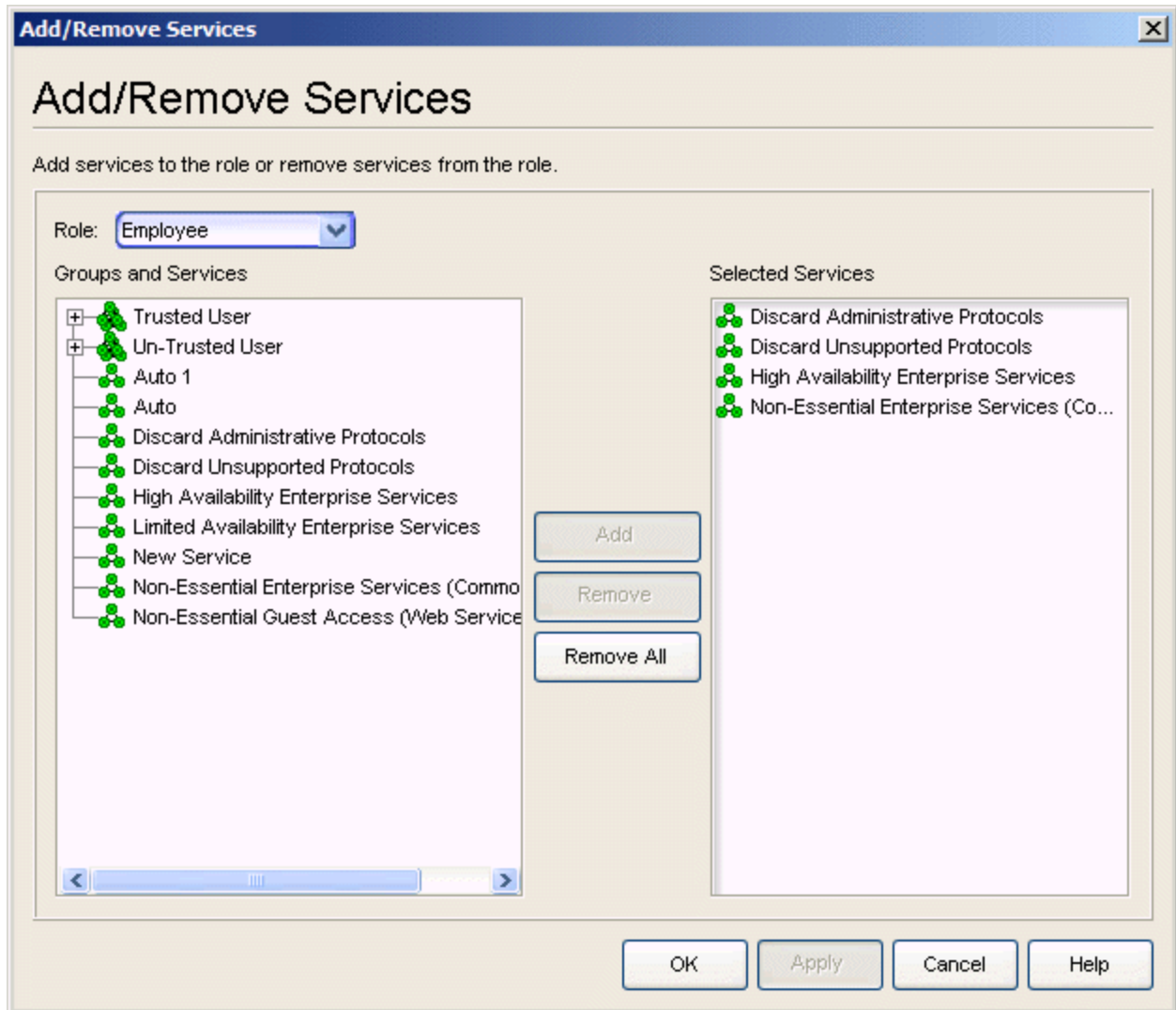
You can add and remove services and service groups from roles using the Add/Remove Services window.

To access the Add/Remove Services window, you must have a role selected in the left-panel Roles tab and the Services tab selected in the right panel. Click the **Add/Remove Services** button.

If you add a service to a role and any or all of the following conditions exist, you are in effect adding an "empty" service, and a warning message will be displayed when you click **OK** or **Apply**:

- No traffic description exists for one or more of the classification rules.
- No access control or class of service has been defined for one or more of the classification rules.
- All of the classification rules are disabled.

When you add a service to a role which already has services associated with it, Policy Manager checks for rule conflicts. See [Conflict Checking](#) for more information.



### Role

Use the drop-down list to select the role where you want to add or remove service groups and services.

### Groups and Services

This field displays all the service groups and services (local and global) in the current domain. [Select](#) the service groups or services you want to add to the role.

### Selected Services

This field displays all the services currently defined for the selected role. [Select](#) the services you want to remove from the role.

### Add Button

Click **Add** to add the services or service groups selected in the Groups and Services field to the Selected Services field. You can also add a service by double clicking the service or using drag and drop.

### Remove Button

Click **Remove** to remove the services selected in the Selected Services field. You can also double click a service to remove it.

### Remove All Button

Click **Remove All** to remove all the services in the Selected Services field.

---

## Related Information

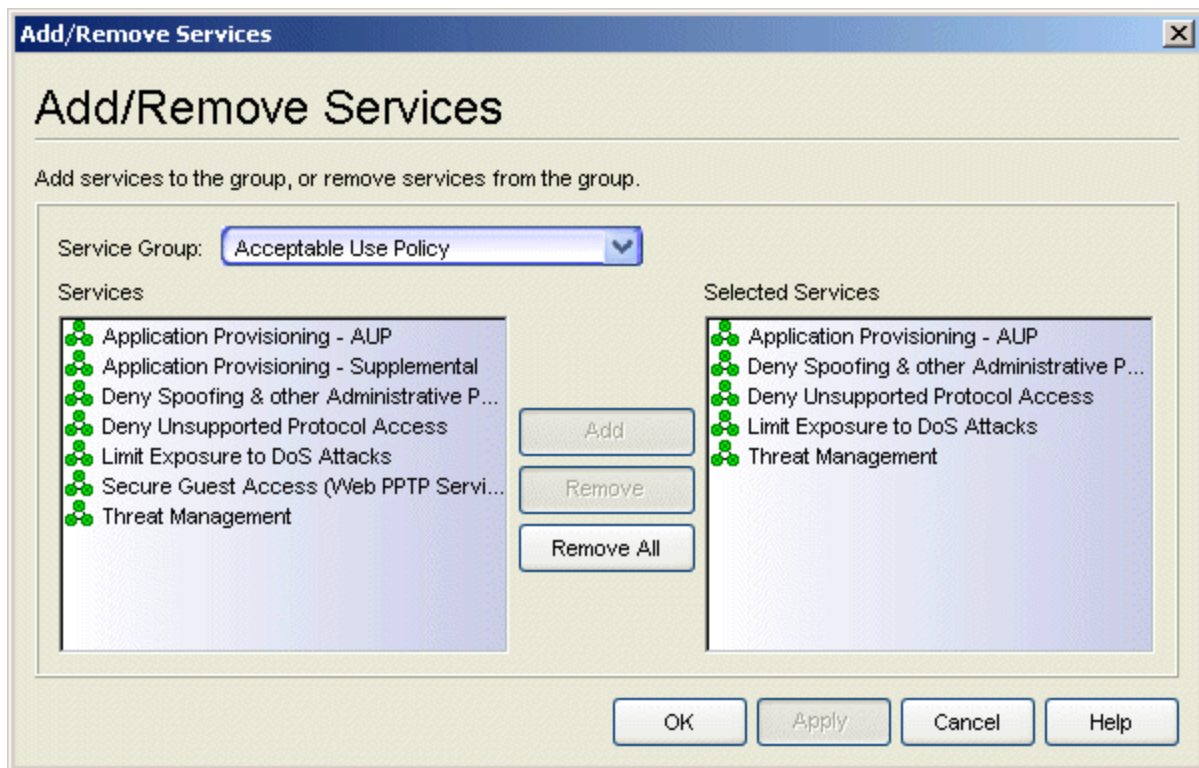
For information on related tasks:

- [Adding Services to a Role](#)
- [Removing Services from a Role](#)

## Add/Remove Services Window (Service Groups)

You can add and remove services from service groups using the Add/Remove Services window.

To access the Add/Remove Services window, you must have a Service Group selected in the left-panel Services tab, then select **Edit > Add/Remove Services**. You can also right-click on a service group and select Add/Remove Services from the menu.



### Service Group

Use the drop-down list to select the service group where you want to add or remove services. The list displays either your local or global service groups, depending whether you launched the window with a local or global service group selected.

### Services

This field displays all the local or global services in the current domain, depending whether you launched the window with a local or global service group selected. [Select](#) the services you want to add to the service group.

### Selected Services

This field displays all the services currently defined for the selected service group. [Select](#) the services you want to remove from the service group.

### Add Button

Click **Add** to add the services selected in the Services field to the Selected Services field. You can also add a service by double clicking the service or using drag and drop.

### Remove Button

Click **Remove** to remove the services selected in the Selected Services field. You can also double click a service to remove it.

### Remove All Button

Click **Remove All** to remove all the services in the Selected Services field.

---

## Related Information

For information on related tasks:

- [Adding Services to a Service Group](#)
- [Removing Services from a Service Group](#)

## Add Static MAC Window

---

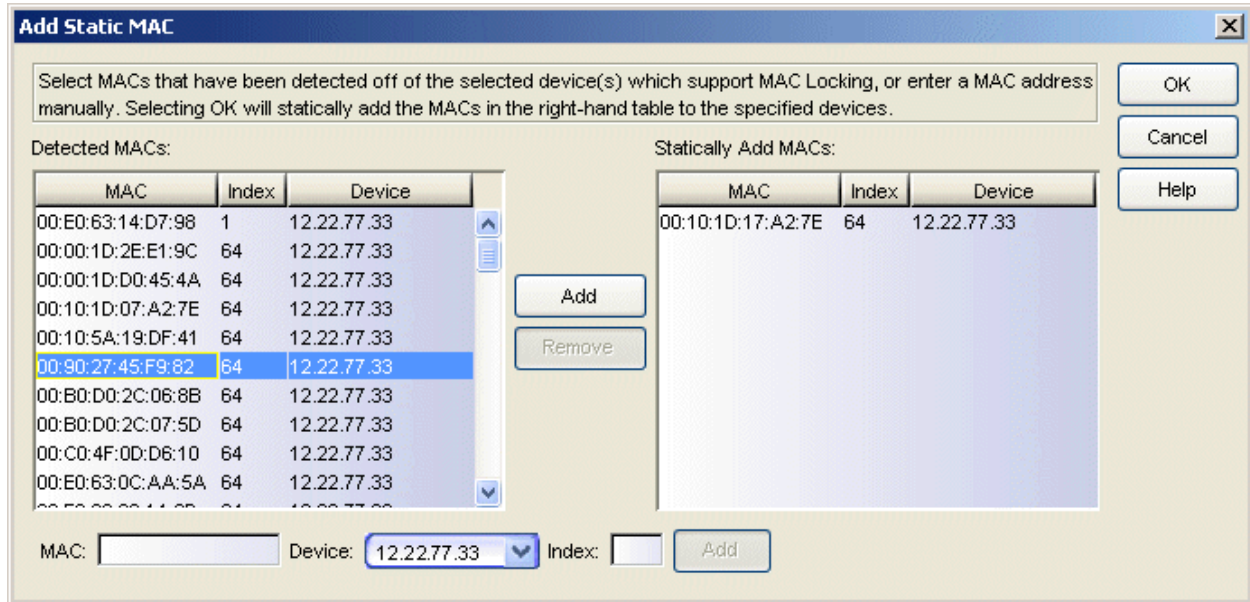
The Add Static MAC window displays current MAC addresses detected on the selected device(s), and lets you create a list of MAC addresses to lock (referred to as Static MAC Locking). MAC Locking ensures that only certain MAC addresses can access a port, and that traffic from any other MAC addresses will be discarded. MAC Locking is only available on devices that support it, and is not allowed on backplane and logical ports.

In order for MAC Locking to take effect on a port, it must be enabled on the port and at the device level. You can enable MAC Locking for a specific port using the [Port Properties MAC Locking Tab](#), or for multiple ports using the [Port Configuration wizard](#). You can enable MAC Locking for a device using the [MAC Locking Tab \(Device\)](#) or the [Device Configuration wizard](#).

To access this window, select a device, device group, or the Devices folder, or a port or port group, in the left-panel Network Elements tab. Select the MAC Locking tab in the right panel, and click **Retrieve** to display the current list of locked MAC addresses for the selected item. Click the **Add** button to open the Add Static MAC window. (If the device does not support the MAC locking feature, the **Retrieve** and **Add** buttons are grayed out.)

If you have selected the Devices folder, a device group, or a port group, the Add Static MAC window looks like the window below. If you selected a single device or port, the tables in the window will not include the Device column and there will be no Device drop-down list.





### Detected MACs

This table displays the MAC addresses detected on the selected device(s) or port group and their corresponding index number and device IP address. (Only MAC addresses for devices that support MAC Locking are displayed.) If you have selected a single device in the left-panel tree, the Device column will not be included. Select the desired MAC address and click **Add** to list the address in the Statically Add MACs list. You can also add a MAC address by double-clicking it.

### Statically Add MACs

Lists the MAC addresses that you want to lock to a specific port or ports. To remove a MAC address from the list, select the address and click **Remove**. If you have selected a single device or port in the left-panel tree, the Device column will not be included.

### MAC/Device/Index

Enter a MAC address and index number, and select a device from the dropdown list (if applicable). Click **Add** to add the address to the Statically Add MACs list. If you have selected a single device or port in the left-panel tree, the device drop-down list is not displayed.

### Add Button

Adds the MAC addresses selected in the Detected MACs table or specified in the fields to the Statically Add MACs table.

### Remove Button

Removes the MAC address selected in the Statically Add MACs table. You can also double click a MAC address to remove it.

### OK Button

Adds the Statically Add MACs list to the Static MAC Locking lists on the devices.

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

For information on related tasks:

- [Using the Device Configuration Wizard](#)
- [Using the Port Configuration Wizard](#)
- [How to Lock MAC Addresses to Ports](#)

For information on related windows:

- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(Devices Folder\)](#)
- [MAC Locking Tab \(Device Group\)](#)
- [Port Properties - MAC Locking Tab](#)
- [MAC Locking Tab \(Port Group\)](#)

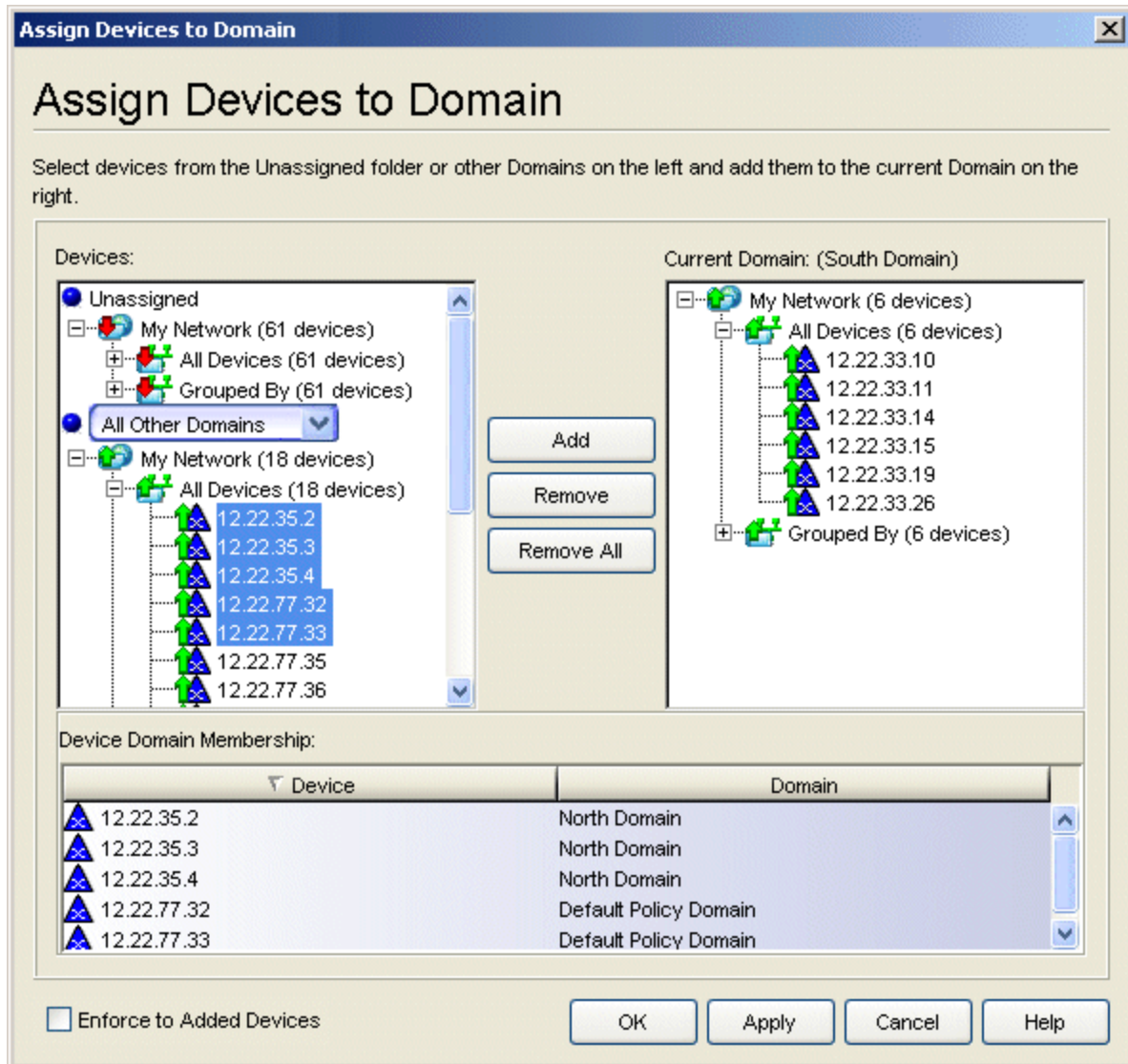
## Assign Devices to Domain Window

---

This window lets you assign devices that are in the NetSight database to a Policy Domain or move devices from one domain to another. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. A device can exist in only one Policy Domain. For more information on domains, see [How to Create and Use Domains](#).

Initially, you must use Console to add your devices to the NetSight database. Once your devices are in the database, you can use this window to assign the devices to a Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy Manager Network Elements tree. Only devices that support policy are displayed in the Policy Manager tree.

To access this window, [open the domain](#) that you want to assign devices to, and select **Domain > Assign Devices to Domain**.



## Devices

The Devices panel displays all the unassigned devices that are in the database (including devices that do not support policy) but are not assigned to a domain. The panel also displays any other domains and the devices assigned to that domain. Use the drop-down list to select a single domain or All Other Domains. If you select All Other Domains, use the bottom panel to view which domain each device is assigned to.

## Current Domain

The right panel displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and click **Add**. You can also select and add multiple devices. To remove a device from the current domain, select the device and click

**Remove.** This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from.

### Device Domain Membership

This section is only displayed when more than one domain exists. It lists the domain assignment for whatever device or device group you have selected in the Devices panel. This is particularly useful when you have selected All Other Domains from the drop-down list in the Devices panel, as it allows you to quickly see the domain assignment for each device.

### Enforce to Added Devices Checkbox

Selecting this checkbox will enforce (write role information) to the devices that are added into the domain when you click **Apply** or **OK**.

### Add Button

Adds the devices selected in the Devices panel to the current domain.

### Remove Button

Removes the devices selected in the Current Domain panel from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from.

---

**NOTE:** Removing a device from a domain does not delete the device from the NetSight database. To [delete a device from the database](#), right-click on the device in the left-panel Network Elements tab, and select **Delete** from the menu. When a device is deleted from the database, it is automatically removed from the Console and Policy Manager device tree.

---

### Remove All Button

Removes all the devices from the current domain.

### OK/Apply Button

Assigns the selected devices to the current domain and displays the devices in the Policy Manager Network Elements tree. Only devices that support policy are assigned to the domain and displayed in the Policy Manager tree.

---

## Related Information

For information on related tasks:

- [How to Add and Delete Devices](#)
- [How to Create and Use Domains](#)

# Class of Service Configuration Window

Use this window to define the Class of Service (CoS) configuration you want to use in the current domain. To access this window, select Class of Service Configuration from the Policy Manager Edit menu.

When you first install Policy Manager, this window is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these predefined classes of service or create your own classes of service.

You can also use this window to define inbound and outbound rate limits and outbound transmit queue rate shapers for your classes of service.

After you have created and defined your classes of service, you can assign them as a classification rule action, a role default, or as part of the definition of an automated service. See [Getting Started with Class of Service](#) and [How to Create a Class of Service](#) for more information.

The screenshot shows the 'Class of Service Configuration (Editable)' window. It features a table with columns for Name, Index, Priority, ToS, Drop Precedence, IRL, ORL, TxQ Shaper, Transmit Queue, Flood Control, Inbound User Based RL, and OUB. The table lists eight predefined classes of service, each with a priority and various configuration options.

Name	Index	Priority	ToS	Drop Precedence	IRL	ORL	TxQ Shaper	Transmit Queue	Flood Control	Inbound User Based RL	OUB
Scavenger [Static]	0	Priorit...					Default	Strict Mode	Disabled	Disabled	
Best Effort [Static]	1	Priorit...						Strict Mode	Disabled	Disabled	
Bulk Data [Static]	2	Priorit...						Strict Mode	Disabled	Disabled	
Critical Data [Static]	3	Priorit...						Strict Mode	Disabled	Disabled	
Network Control [Static]	4	Priorit...						Strict Mode	Disabled	Disabled	
Network Management [Static]	5	Priorit...						Strict Mode	Disabled	Disabled	
RTP/Voice/Video [Static]	6	Priorit...	Low					Strict Mode	Disabled	Disabled	
High Priority [Static]	7	Priorit...						Strict Mode	Disabled	Disabled	
Redirect to nacdemo	8	None	60:ff					Strict Mode	Disabled	Disabled	
NAC Web Redirect	9	Priorit...	40:ff					Strict Mode	Disabled	Disabled	

## Create Menu

Use the Create menu to create a new class of service, or a new rate limit or transmit queue rate shaper port group. For more information on port groups, see [Creating Class of Service Port Groups](#).

### Table Display Filter

Use this menu to specify which CoS component columns you would like displayed in the table. For example, if you want to view the inbound rate limits that are configured, you can select to display only Inbound RL, making it easier for you to focus in on the desired information. You can also filter by port group name. For example, if you have created two port groups named Edge and Core for your Inbound RL, Outbound RL, and TxQ Shapers, selecting Core from the menu will display only the IRL/ORL/TxQ settings for the Core group in the table.

### Domain Managed CoS Components

Use this menu to specify the CoS components you will be configuring for this domain. This will determine what CoS settings will be written to your network switches on Enforce. For example, if you select only Inbound RL and Outbound RL, then Policy Manager will enforce the rate limits you configure, but will not overwrite any transmit queue settings configured on the device via the Command Line Interface (CLI).

Use the **Show all CoS components in tree (Advanced Mode)** option to display the individual CoS components in a left-panel tree. The Advanced Mode allows you to change the rate limit and transmit queue [index numbers](#) associated with the class of service, as well as map different rates to different port types in your [rate limit port groups](#).

---

**TIP:** For many of the values below, hovering over the value in the table will show a tooltip with more information about the current settings.

---

#### Name

The name of the class of service.

#### Index

The index number automatically assigned to the class of service.

#### Priority

The 802.1p priority associated with the class of service. Double-click a priority to select a new priority, if desired. The priority for the eight static classes of service provided by Policy Manager (Priority 0-7), cannot be disabled or changed.

#### ToS

The IP type of service value associated with this class of service, if any. See [IP Type of Service](#) for more information. Double-click in the ToS column to enter a ToS value or open the [ToS/DSCP Configuration window](#).



### Drop Precedence

The [drop precedence](#) associated with this class of service. Double-click in the column to select a Drop Precedence value: Low, Medium, or High.

### Inbound RL

The port inbound rate limit (IRL) that is configured for the Default port group, if any. If you have created additional port groups, the rate limits will be displayed for those groups as well. Double-click in the column to set or change a rate for each class of service. Right-click on the Inbound RL column heading to create a new Inbound RL port group. Then, right-click on the port group name to open the [Add/Remove Ports window](#) to assign which port will be in each group.

### Outbound RL

The port outbound rate limit (ORL) that is configured for the Default port group, if any. If you have created additional port groups, the rate limits will be displayed for those groups as well. Double-click in the column to set or change a rate for each class of service. Right-click on the Outbound RL column heading to create a new Outbound RL port group. Then, right-click on the port group name to open the [Add/Remove Ports window](#) to assign which port will be in each group.

### TxQ Shaper

The rate shaper that is configured for the Default port group, if any. If you have created additional port groups, the rate shaper will be displayed for those groups as well. Double-click in the column to set or change a rate for each class of service. Right-click on the TxQ Shaper column heading to create a new TxQ Shaper port group. Then, right-click on the port group name to open the [Add/Remove Ports window](#) to assign which port will be in each group.

### Transmit Queue

The Queue column displays the transmit queue associated with the class of service for each port type. Double-click the queue to see a drop-down menu where you can select a new transmit queue, if desired. The Bandwidth column displays the [arbiter mode configuration](#) for all queues. Double-click the Bandwidth column to open the [Edit Bandwidth Configuration Window](#) where you can configure the arbiter mode for all queues. If you have used advanced mode to configure different arbiter modes for multiple transmit queue port groups, the Bandwidth column will display "Advanced".

### Flood Control

The Flood Control column displays the rate limit for incoming traffic configured for each of the following traffic types (unknown-unicast,

broadcast, or multicast). While Flood Control rates can be changed by editing a cell for a class of service, these rates are shared globally by all CoS in the domain. All Flood Control enabled CoS will share these rates. When Flood Control configuration is edited, all affected CoS will have their cells highlighted. Double-click in the column to set or change the rate for each type. To leave the Flood Control rates and just enable or disable Flood Control for a CoS, select Enable or Disable Flood Control from the drop-down menu.

---

**NOTE:** By default, Flood Control is not managed by Policy Manager. To manage flood control configuration on devices in a domain, it can be enabled via the Domain Managed CoS Components drop-down menu by selecting All CoS Components or by selecting Flood Control.

---

### Inbound User Based RL

If you have ExtremeWireless Wireless Controllers on your network, this column displays the inbound rate limit that is configured for the Default port group, if any. Double-click in the column to set or change a rate for each class of service. Currently, user-based rate limits are only available for wireless controllers.

### Outbound User Based RL

If you have ExtremeWireless Wireless Controllers on your network, this column displays the outbound rate limit that is configured for the Default port group, if any. Double-click in the column to set or change a rate for each class of service. Currently, user-based rate limits are only available for wireless controllers.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)

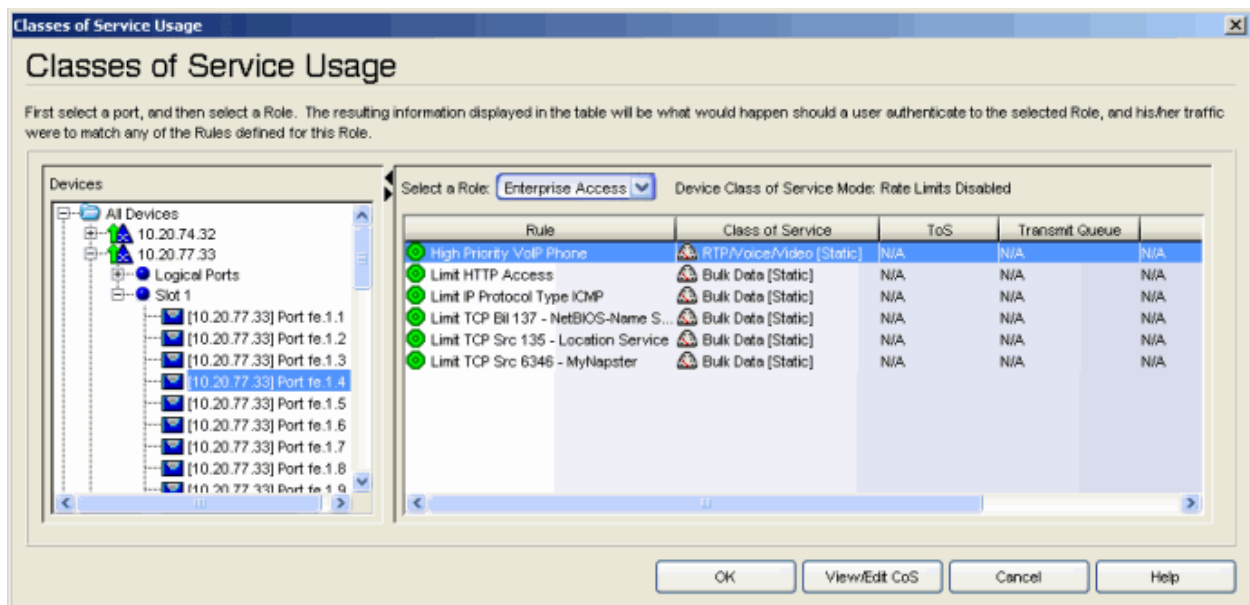
For information on related windows:

- [General Tab \(Class of Service\)](#)

## Classes of Service Usage Window

This window provides an easy way to view class of service information for a specific port. In the window, you select a port and a role. A table then displays the actual rate limit and transmit queue configuration that would be implemented on the selected port if a user's traffic were to match any of the rules defined for the role.

To access this window, select **View > CoS Usage** from the menu bar. You can also access the window by right-clicking a port in the left-panel Network Elements tab and selecting CoS Usage from the menu. The port will be automatically selected in the window.



### Devices

Expand the tree and select the port whose class of service usage you want to view.

### Select a Role

Use the drop-down list to select the desired role.

### Device Class of Service Mode

The Class of Service mode specified for the device on the [device General tab](#).

**Rule**

The name of the rule the class of service is part of.

**Class of Service**

The name of the class of service associated with the rule.

**ToS**

The ToS value associated with the class of service, if any.

**Transmit Queue**

The transmit queue associated with the class of service for this port.

**Inbound Rate Limit**

The inbound rate limit associated with the class of service for this port.

**View/Edit CoS Button**

Select a rule in the table and click this button to access the class of service (CoS) General tab where you can view and edit the class of service values.

---

**Related Information**

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

For information on related windows:

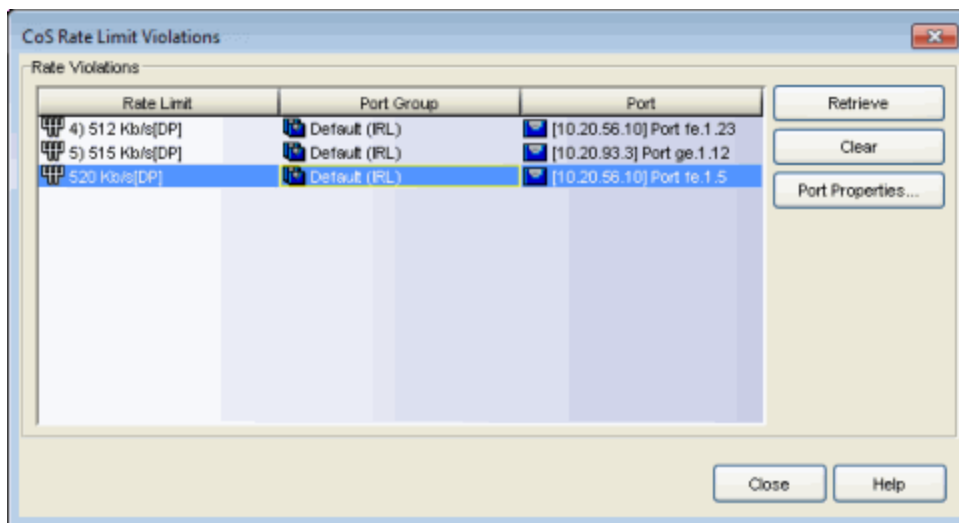
- [General Tab \(Class of Service\)](#)

## CoS Rate Limit Violations Window

This window displays rate limits where traffic has exceeded the configured limit for a port and a violation has occurred. There are two ways to access this window:

**To view all rate limit violations:** Open the [Class of Service Configuration Window](#) (available from the Policy Manager Edit menu) and click the **Rate Violations** button.

**To view rate limit violations for a specific Class of Service:** Open the [Class of Service Configuration Window](#), right-click a CoS where one or more rate limits have been assigned, and select **CoS Rate Limit Violations** from the menu



### Rate Limit

Displays the rate limits where traffic has exceeded the configured limit.

### Port Group

Displays the port group that includes the port where the rate violation occurred.

### Port

Displays the name of the port where the rate limit violation occurred. The port name is constructed of the name or IP address of the device and either the port index number or the port interface name.

### Retrieve Button

Depending on how you have accessed the window, this button retrieves rate limit violation information from all the ports in the domain or from ports where the selected CoS is assigned via a role.

### Clear Button

Use this button to clear the selected violation off the device.

### Port Properties

Select a port in the table and click this button to open the [Port Properties window](#) where you can view and edit port information.

---

### Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Define Rate Limits](#)

## Create Class of Service Window

This window lets you create a class of service (CoS) that includes one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, rate limits, and transmit queue configuration. Once you've created the class of service, you can apply it as a classification rule action, as part of the definition of an automated service, or as a role default. For more information, see [Getting Started with Class of Service](#).

To access this window, open the [Class of Service Configuration Window](#) (available from the Policy Manager Edit menu). Then, click the **Create** button and select Create Class of Service from the menu.

The screenshot shows the 'Create Class of Service' dialog box. The 'Name' field contains 'Web Redirection'. The 'General' section has a checked '802.1p Priority' dropdown set to 'Priority 6'. 'ToS/DSCP Marking' is unchecked, with 'Value 0x' and 'Mask 0x' fields. 'Drop Precedence' is set to 'None'. 'Transmit Queue' is set to 'Transmit Queue 3'. The 'Rate Limit Configuration' section has 'Inbound Rate Limit' and 'Inbound User Rate Limit' both set to '2) 5 Mb/s', and 'Outbound Rate Limit' and 'Outbound User Rate Limit' both set to 'None'. Buttons for 'OK', 'Apply', 'Cancel', and 'Help' are on the right.

### Name

Enter the name of the class of service.

## General

### 802.1p Priority

If the class of service includes an 802.1p priority, select this checkbox and use the drop-down list to choose the priority (0-7 with 7 being the highest priority).

### ToS/DSCP Marking

Some IP rules allow a ToS/DSCP value to be written to the ToS/DSCP field in the IP header of incoming packets. Select this option to associate an IP ToS (Type of Service) or DSCP (Diffserv Codepoint) rewrite value with this class of service. See [ToS/DSCP Rewrite](#) and [ToS/DSCP Value Definition Chart](#) for more information.

- **Value** - The IP type of service value is an 8-bit hexadecimal number between 0 and FF (see [IP Type of Service](#) for more information). You can either enter this value in the **Value Ox** text box, or click **Select** to open the [ToS/DSCP Configuration window](#), where you can automatically configure a ToS (Type of Service) or DSCP (Diffserv Codepoint) value.
- **Mask** - The ToS mask controls which bits in the ToS/DSCP field of incoming packets will be overwritten. Masking a ToS value is only supported on K-Series, S-Series and N-Series devices. Devices that do not support the mask will ignore this field.

---

**NOTE:** If you apply a class of service with a ToS/DSCP value as a role default, the ToS/DSCP value will be ignored. This is because ToS/DSCP rewrite works only for certain IP ToS classification rules, not as a role default.

---

### Drop Precedence

The Drop Precedence option is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence will dictate the internal priority (within the MAC chip) that will be used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.

### Transmit Queue

Use the drop-down menu to select a transmit queue for the class of service. If you would like to select a different transmit queue for each port type, select the "Q/Port Type" option. Then, when you click **Apply** or **OK**, you will see a window where you can specify a different transmit queue for each port type.



## Rate Limit Configuration

This section lets you select the port inbound and outbound rate limit to associate with the class of service.

Rate limits are used to control the transmit rate at which traffic enters and exits ports in your network. All traffic mapped to this Class of Service on a given port will share the bandwidth specified by the rate limit.

In addition, if you have ExtremeWireless Wireless Controllers (Release 8.01.xx or higher) on your network, you will see an option to configure inbound and outbound user rate limits. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for these wireless controllers.

### Inbound/Outbound Rate Limit

Use the drop-down list to select or create the port inbound/outbound rate limit to associate with the class of service.

### Inbound/Outbound User Rate Limit

Use the drop-down list to select or create the user inbound/outbound rate limit to associate with the class of service.

---

## Related Information

For information on related concepts:

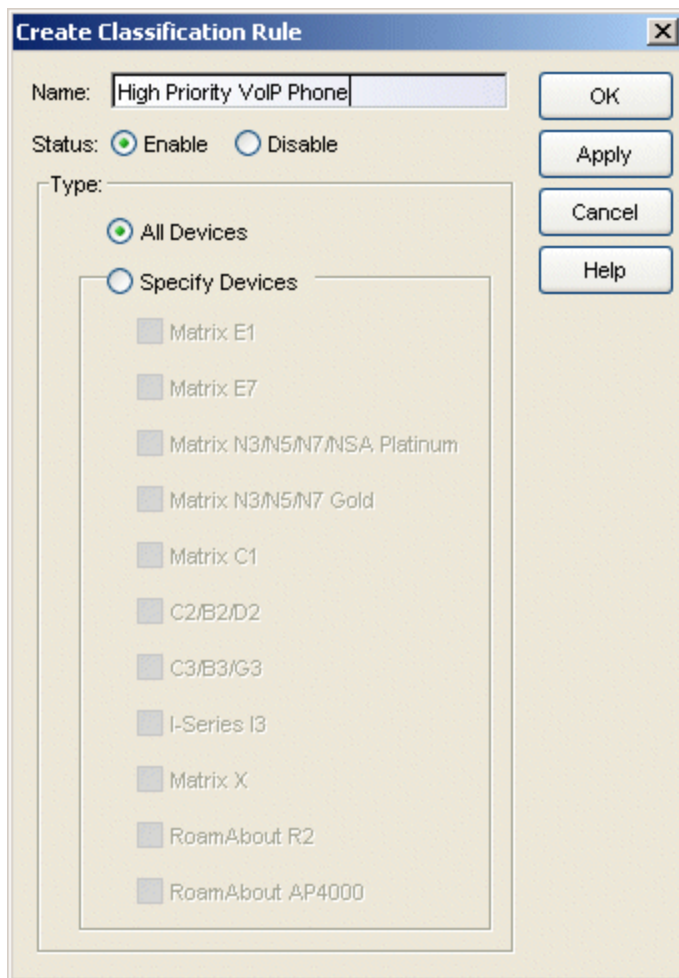
- [Getting Started with Class of Service](#)
- [IP Type of Service](#)

For information on related tasks:

- [How to Create a Class of Service](#)
- [How to Define Rate Limits](#)
- [How to Configure Transmit Queues](#)

## Create Classification Rule Window

This window appears when you select a service in the left-panel Services tab and select the Create Classification Rule right-click menu option. It provides a way to add a rule to a service without using the Classification Rule Wizard. If you use this window, traffic descriptions and actions can be added to the rule afterwards (see [Using the Rule Tabs](#)). In order for a rule to be applied to devices, you must [enforce](#).



The screenshot shows a dialog box titled "Create Classification Rule". It has a text input field for "Name" containing "High Priority VoIP Phone". Below it, "Status" is set to "Enable" with a selected radio button. Under "Type", "All Devices" is selected with a radio button. A list of devices is shown under "Specify Devices", each with an unchecked checkbox: Matrix E1, Matrix E7, Matrix N3/N5/N7/NSA Platinum, Matrix N3/N5/N7 Gold, Matrix C1, C2/B2/D2, C3/B3/G3, I-Series I3, Matrix X, RoamAbout R2, and RoamAbout AP4000. On the right side, there are four buttons: OK, Apply, Cancel, and Help.

### Name

Enter a name for the rule.

### Status

Disable the rule, if desired. If a rule is disabled, it is unavailable for use by the current service, but can still be copied to other services and enabled, or

re-enabled at another time on the rule's [General tab](#). The rule icon in the left panel displays a red X if the rule is disabled.

### Type

Select the types of devices to which you wish this rule to apply when enforced. See [Rule Type](#) for more information on the consequences of your choice.

---

### Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [Using the Rule Tabs](#)

For information on related windows:

- [General Tab \(Rule\)](#)

## Create Mixed-Stack C2/C3 Domain Tool

---

This tool provides a way to manage mixed stacks of C2/C3 and B2/B3 devices by creating a new domain specifically for those mixed stack devices, using the data in the currently active domain. This is necessary because C3 and B3 devices do not support Class of Service rate limiting and certain rule types (Layer 2 rules and ICMP Layer 3 rules) that are supported by the C2 and B2 devices. When you have a mixed stack, all devices in the stack have the rule type and Class of Service limitations of the C3 or B3 device, despite the fact that the stack may report itself as a C2 or B2 device. (The device type that the stack reports is based on what switch is set as the master. It is strongly recommended that the C3 or B3 device be configured as the master in the mixed stack) Because of the C3 and B3 limitations, managing a mixed stack in a domain with C2 or B2 rules in use, will cause enforce to fail. For more information on mixed stack limitations, see [Mixed-Stack C2/C3 and B2/B3 Considerations](#) in the Policy Manager Configuration Considerations.

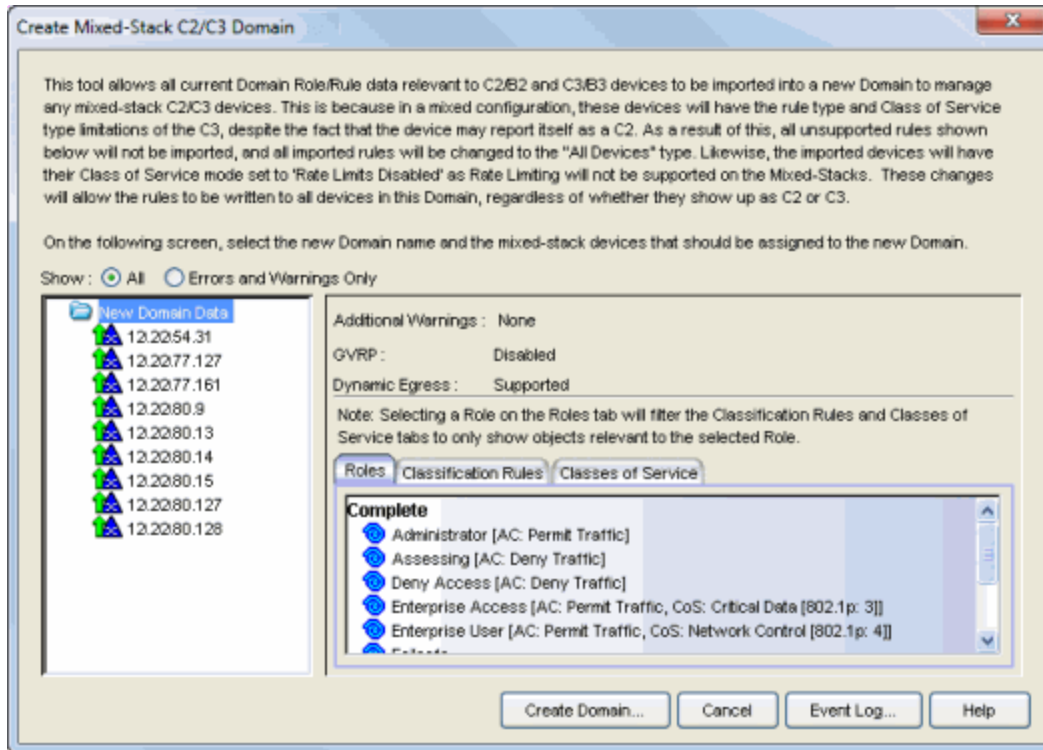
Using this tool, you can import all current domain role/rule data relevant to your mixed stack devices into a new domain created specifically to manage those mixed stacks. Unsupported rules (Layer 2 rules and ICMP Layer 3 rules) are not imported, and all imported rules are changed to the "All Devices" type. In addition, the imported devices will have their Class of Service mode set to "Rate Limits Disabled" because rate limiting is not supported in mixed stacks. These changes allow the rules to be enforced to all devices in the new domain, regardless of what type of device they are reporting as.

---

**NOTE:** After you have created your new mixed-stack domain, be careful not to add unsupported rules to the new domain or enforce will once again fail.

---

You can access the tool from the **Domain > Create Mixed-Stack C2/C3/B2/B3 Domain** menu option. The tool has two windows. The first window lets you view the configuration data that will be imported into the new domain. When you click **Create Domain** in that window, the second window opens where you select the specific devices that you want to include in the new mixed-stack domain. When you click **OK** in that window, a new mixed-stack domain is created and opened.



## "Show" Radio Buttons

These radio buttons determine the amount of data displayed in the right panel of the window.


### All

Select this radio button to display what will *and* what will not be imported into the new domain.

### Errors and Warnings Only

Select this radio button to show only what will *not* be imported into the new domain.

## Left Panel

The left panel of the window displays a New Domain Data folder that contains the C2/C3 and B2/B3 devices in your network. The  icon alerts you that there are certain things that will not be imported into the new domain.

## Right Panel

The upper portion of the right panel provides information about whether certain policy management features are supported and/or enabled for the devices listed in the left panel.

- **Additional Warnings** - This section notifies you if there are problems detected with the policy configuration. View the Enforce Warnings in the Event Log for details.
- **GVRP** - Shows whether GVRP is Enabled, Disabled, or Ignored. You can change GVRP status for the domain via the Edit menu.
- **Dynamic Egress** - Shows whether [Dynamic Egress](#) is Supported or Not Supported.

There are three tabs that provide specific information about the roles, classification rules, and classes of service that will be imported into the new domain. The information displayed depends on whether you have the [Show All](#) or the [Show Errors and Warnings Only](#) radio button selected. In addition, you can select a role in the Roles tab to filter the information for just that role.

### Roles Tab

**Incomplete** - Lists any roles with unsupported classification rules that will not be imported. These roles will be imported to the new domain, but without the unsupported rules.

**Complete** - Lists any roles which do *not* include unsupported classification rules. These roles will be imported as defined.

### Classification Rules Tab

**Excluded** - Lists any unsupported classification rules (Layer 2 rules and ICMP Layer 3 rules) that have been applied to a role. These rules will not be included when the associated roles are imported to the new domain.

**Included** - Lists any supported classification rules that have been applied to a role. These rules will be included when the associated roles are imported to the new domain.

### Classes of Service Tab

**Class of Service Mode** - Lists the Class of Service mode currently in effect on the devices. The Class of Service mode will always be set to "Rate Limits Disabled" for the devices in the new mixed-stack domain.

**Classes of Service Subtab** - Lists the classes of service that will be imported to the new domain:

- Class of Service - the name of the class of service.
- 802.1p Priority - the priority associated with the class of service.
- ToS Value - the IP type of service value associated with this class of service, if any. See [IP Type of Service](#) for more information.
- TxQueue Index - the transmit queue index associated with the class of service.
- IRL Index - the role-based inbound rate limit index associated with the class of service.
- ORL Index - the role-based outbound rate limit index associated with the class of service.

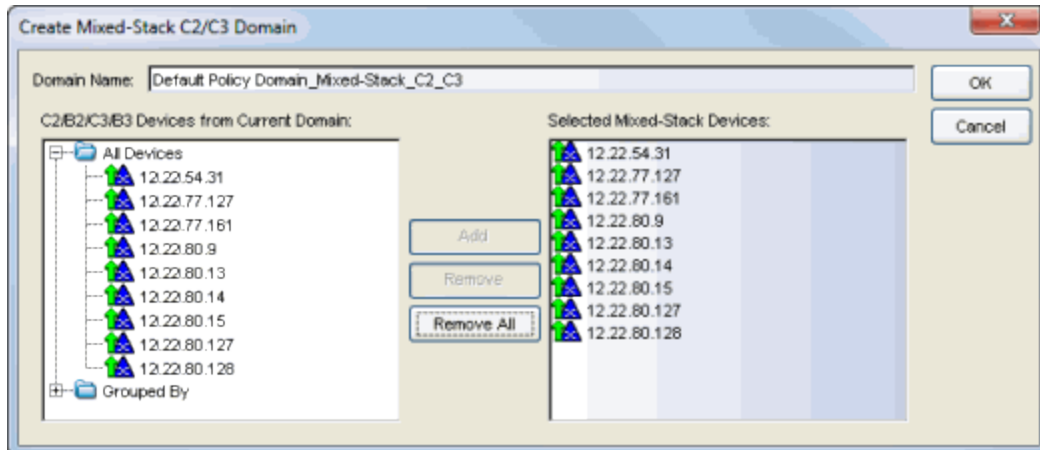
For more information, see [Getting Started with Class of Service](#) and [How to Create a Class of Service](#).

**Inbound/Outbound Role-Based Rate Limit Mappings Subtabs** - Lists the rate limit mappings that will be imported to the new domain:

- Device - The device where the rate limit mapping is in effect.
- IRL/ORL Port Grp - The name of the port group that contains the rate limit mapping.
- IRL/ORL Index - The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming packets.
- Rate Limit - The actual rate limit that the IRL/ORL index is mapped to.
- IRL/ORL Port Type - The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).
- Information - Information about mapping support.

### Create Domain Button

Opens the second window of the tool where you can select the mixed-stack devices you want included in the new domain. In most cases, you should create one new domain for the mixed-stack devices in each of your domains.



### Domain Name

Use this field to enter a name for the new domain or use the default name that's displayed.

### C2/B2/C3/B3 Devices from Current Domain

This panel lists the C2/C3 and B2/B3 devices in the current domain. Select the devices that will be included in the mixed-stacks and click **Add**. (In most cases, you should create one new domain for the mixed-stack devices in each of your domains.)

### Selected Mixed-Stack Devices

This panel lists the devices you've selected for the mixed-stack domain. To remove a device, select the device and click **Remove**, or click **Remove All** to remove all devices from the list.

### OK Button

Creates and opens a new domain for your mixed-stack devices.

---

## Related Information

For information on related concepts:

- [Policy Domains](#)
- [Traffic Classification Rules](#)



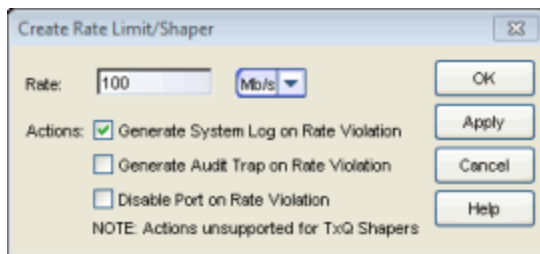
## Create Rate Limit/Shaper Window

---

This window allows you to create and define a [rate limit](#). Rate limits are components of a Policy Manager class of service, and are used to control the transmit rate at which traffic enters and exits ports in your network.

To access this window, open the [Class of Service Configuration Window](#) (available from the Policy Manager Edit menu). Click on the **Domain Managed CoS Components** button and select the **Show all CoS Components in Tree (Advanced Mode)** menu option. Right-click the Rate Limits folder in the left-panel tree, and select the Create Rate Limit option.

To create the rate limit, fill out the window and click **OK** (to create a single rate limit) or **Apply** (to create more rate limits). After you create the rate limit, the General tab for the new rate limit appears, where you can configure additional rate limit parameters.



### Rate Limit

Specify the highest transmission rate at which traffic can enter or exit a port before packets will be rate limited:

- % - A percentage of the total bandwidth available (not available for priority-based rate limits)
- PPS - Packets per second (not available for priority-based rate limits)
- Kb/s - Kilobits per second
- Mb/s - Megabits per second
- Gb/s - Gigabits per second

### Actions

Select the action(s) you would like this rate limit to use:

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

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

---

**NOTE:** N-Series Gold devices do not support rate limit notification.

---

## Related Information

For information on related concepts:

- [Rate Limits](#)

For information on related tasks:

- [How to Define Rate Limits](#)

## Create VLAN Window

---

This window appears when you select the Create VLAN menu option, or if you select **New** in the [VLAN Selection View](#) or the Role VLAN window in the Role Wizard. See [How to Create a VLAN](#), [How to Create a Policy VLAN Island](#), and [Roles](#) for additional information.

### VLAN Name

The name for the VLAN you want to create. VLAN names can be up to 32 characters in length, including spaces. Do not create a VLAN name that uses any letters with diacritical marks. Diacritical marked letters are not supported by SNMP. VLAN names are case sensitive. For example, "Sales" and "sales" would be considered two different VLAN names. You can have multiple VLANs with the same name but with different VLAN IDs in Policy Manager.

### VLAN ID

Unique numerical identifier for the VLAN, also known as VID. Can be a value between 1 and 4094, with VID1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a default VLAN you assign to a role). To select the next VID in sequence, click **Next Available VID**.

**This VLAN is intended as a Discard VLAN only**

If this VLAN is to be used to deny traffic, select this box. If it is to be used to contain traffic, leave the box unchecked.

**Dynamic Egress Enabled**

Dynamic Egress is enabled by default in Policy Manager. If you want to disable Dynamic Egress, uncheck the box. If you select "This VLAN is intended as a Discard VLAN only" option, the Dynamic Egress Enabled checkbox is automatically deselected. If for some reason you wish to have it enabled for a discard VLAN, you can reselect it. See [Dynamic Egress](#) for more information.

**Always write VLAN to device(s)**

If the box is checked, the VLAN will be written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN will not be written to the device unless it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it allows you to configure that VLAN for Dynamic Egress.

**Next Available VID Button**

Enters the next unassigned [VID](#) in the **VLAN ID** field.

**Apply Button**

Creates the VLAN and leaves the window open.

---

**Related Information**

For information on related concepts:

- [Dynamic Egress](#)
- [Policy VLAN Islands](#)

For information on related tasks:

- [How to Create a VLAN](#)
- [How to Create a Policy VLAN Island](#)

For information on related windows:

- [General Tab \(Role\)](#)

## Device Configuration Wizard Add RADIUS Accounting Server Window

This window lets you add a RADIUS server to Policy Manager for the purpose of RADIUS accounting. Access this window by clicking **Add** in the RADIUS Accounting Server(s) window in the Device Configuration Wizard.

The screenshot shows a window titled "Device Configuration Wizard" with a sub-title "Add RADIUS Accounting Server". Below the title, there is instructional text: "Enter server configuration data. Press 'OK' to add, or 'Cancel'." and "Note: It is recommended that the Server Shared Secret be at least 16 characters." Below this, a note states: "Only Wireless Controllers support and require a per-server update interval value. All other devices support only client default." The main form area contains several input fields: "IP Address:" (empty), "Client UDP Port:" (1813), "Timeout Duration (2-10 sec):" (5), "Number of Retries (0-20):" (5), "Update Interval (min):" with radio buttons for "Client Default" (selected) and "Specify:" (empty), "Server Shared Secret:" (empty), and "Verify Shared Secret:" (empty). At the bottom right of the form area are "OK" and "Cancel" buttons. At the very bottom of the window are navigation buttons: "< Back", "Next >", "Cancel", and "Help".

### IP Address

Enter the IP or IPv6 address of the RADIUS accounting server. Not all devices support IPv6 address types.

### Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send accounting requests to the RADIUS server; 1813 is the default port number.

### Timeout Duration (2 -10 sec)

The amount of time in seconds the device will wait for the RADIUS server to respond to an accounting request. Valid values are 2-10 seconds.

### Number of Retries (0-20)

The number of times the device will resend an accounting request if the RADIUS server does not respond. Valid values are 0-20.

### Update Interval (minutes)

The Update Interval is the amount of time in minutes between accounting updates. For ExtremeWireless Wireless devices, this value is configured here for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Accounting Client Settings](#) section of the RADIUS tab. Devices that do not support RADIUS accounting will have this field grayed out.

### Server Shared Secret

A string of characters used to encrypt and decrypt communications between the RADIUS client (device) and the RADIUS server. This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

**NOTE:** This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and Policy Manager.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

### OK Button

Saves the settings and returns you to the RADIUS Accounting Server(s) window in the Device Configuration Wizard. The new RADIUS server is displayed in the table of servers.

**Cancel (upper) Button**

Returns you to the RADIUS Accounting Server(s) window in the Device Configuration Wizard without saving any settings.

**Cancel (lower) Button**

Exits you from the Device Configuration Wizard without saving any of the settings you've entered so far.

---

**Related Information**

For information on related windows:

- [RADIUS Tab \(Device\)](#)

For information on related tasks:

- [How to Configure Devices](#)

## Device Configuration Wizard Add RADIUS Authentication Server Window

This window lets you add a RADIUS server to Policy Manager for the purpose of authentication. Access this window by clicking **Add** in the RADIUS Authentication Server(s) window in the Device Configuration Wizard

The screenshot shows a window titled "Device Configuration Wizard" with a sub-title "Add RADIUS Authentication Server". Below the title, there is a note: "Enter server configuration data. Press 'OK' to add, or 'Cancel'. Note: It is recommended that the Server Shared Secret be at least 16 characters. Only Wireless Controllers support and require per-server retry and timeout values. All other devices support only client default." The form contains the following fields and options:

- IP Address: [Empty text box]
- Client LDP Port: [1812]
- Max Sessions (Sticky Round-Robin): [2048]
- Number of Retries:  Client Default  Specify (1-10): [Empty text box]
- Timeout Duration (sec):  Client Default  Specify (1-60): [Empty text box]
- Server Shared Secret: [Empty text box]
- Verify Shared Secret: [Empty text box]
- Access Type: [Any access]

At the bottom right of the form area are "OK" and "Cancel" buttons. At the bottom of the window are navigation buttons: "< Back", "Next >", "Cancel", and "Help".

### IP Address

Enter the IP or IPv6 address of the RADIUS authentication server. Not all devices support IPv6 address types.



### Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send authentication requests to the RADIUS authentication server; 1812 is the default port number.

### Max Sessions (Sticky Round-Robin)

Specifies the maximum number of sticky round-robin authentication sessions allowed on the server when the [sticky round-robin RADIUS authentication algorithm](#) is configured for a device. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to. Devices that do not support this functionality will have the option grayed out.

### Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless Wireless devices, this value is configured here for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section of the RADIUS tab.

### Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless Wireless devices, this value is configured here for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the [RADIUS Authentication Client Settings](#) section of the RADIUS tab.

### Server Shared Secret

A string of characters used to encrypt and decrypt communications between the RADIUS client (device) and the RADIUS server. This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate, and authentication attempts will fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

**NOTE:** If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most Policy Manager devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

**NOTE:** This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and Policy Manager.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

### Access Type

Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- **Any access** - the server can authenticate users originating from any access type.
- **Management access** - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

This feature allows you to have one set of servers for authenticating management access requests and a different set for authenticating network access requests.

### OK Button

Saves the settings and returns you to the RADIUS Authentication Server(s) window in the Device Configuration Wizard. The new RADIUS server is displayed in the table of servers.

### Cancel (upper) Button

Returns you to the RADIUS Authentication Server(s) window in the Device Configuration Wizard without saving any settings.

### Cancel (lower) Button

Exits you from the Device Configuration Wizard without saving any of the settings you've entered so far.

---

## Related Information

For information on related concepts:

- [Authentication](#)

For information on related windows:

- [RADIUS Tab \(Device\)](#)

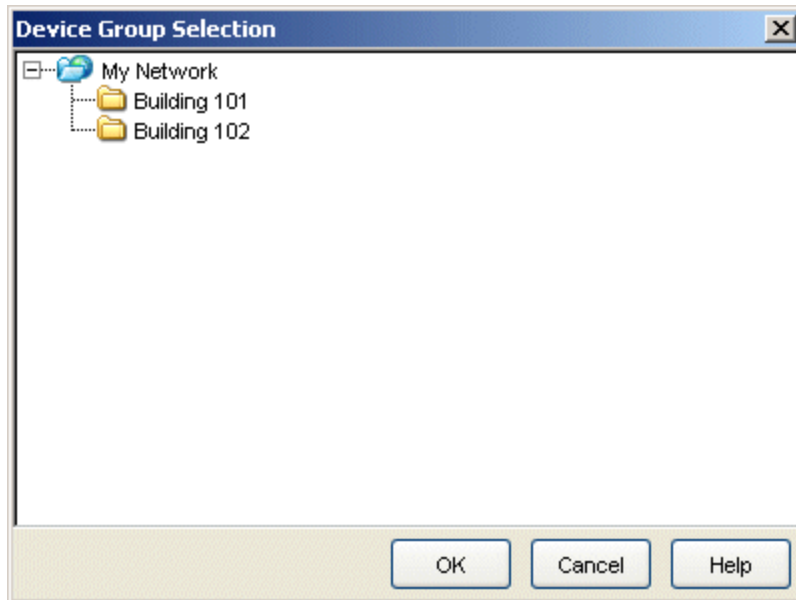
For information on related tasks:

- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)

## Device Group Selection Window

---

The Device Group Selection window lets you add one or more devices from a right-panel Details View to the My Network Group or a user-created group in the left-panel Network Element tab. See [Adding Devices to a Device Group](#) for more information.



### Group Selection Panel

Use this panel to select the group to which you want to add the selected devices.

### OK Button

Adds the device(s) to the selected group.

### Cancel Button

Closes the window without adding any devices.

---

## Related Information

For information on related tasks:

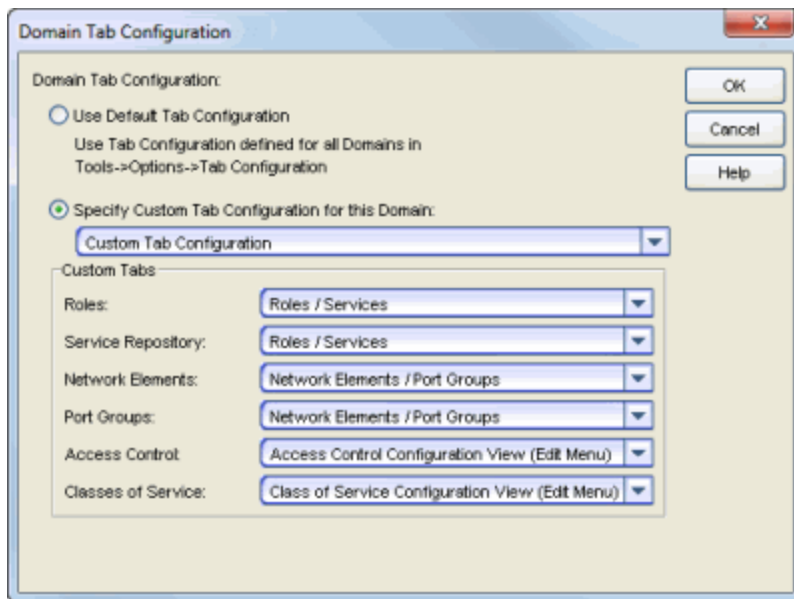
- [How to Add and Remove Device Groups](#)

## Domain Tab Configuration Window

---

The trees in the Policy Manager left panel tabs can be organized into different "tab configurations." The default tab configuration used by all domains is defined in Tools > Options > Tab Configuration. The Domain Tab Configuration window allows you to override the default tab configuration and specify a custom tab configuration for the current domain that is open.

To access this window, select View > Domain Tab Configuration.



### Use Default Tab Configuration

Use the default tab configuration defined for all domains in Tools > Options > Tab Configuration.

### Specify Custom Tab Configuration for this Domain

Use the drop-down list to select the custom tab configuration you would like to use in the current domain:

- Consolidated Tab Configuration (Recommended) - In this configuration, there are two top-level tabs: Roles/Services and Network Elements/Port Groups. Access Control and Class of Service trees are presented in external Configuration windows accessed from the Edit menu.
- Classic Tab Configuration - This configuration uses six top-level tabs, one for each Policy Manager tree: Roles, Services, Access Control,

Classes of Service, Network Elements, and Port Groups. This is similar to the configuration used in Policy Manager prior to version 4.0.

- Custom Tab Configuration - This configuration allows you to define which tab the different Policy Manager trees will be organized under. For Access Control and Classes of Service trees, you can also select to display the tree in a Configuration View (an external window) accessed from the Edit menu.
- 

### **Related Information**

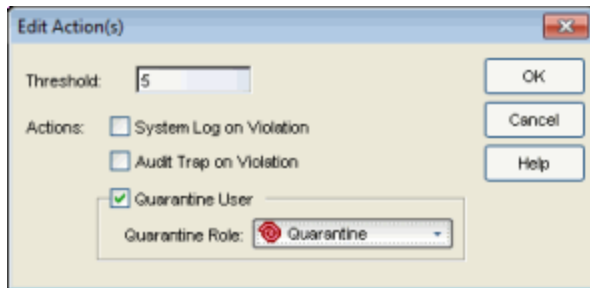
For information on related windows:

- [Tab Configuration Option](#)

## Edit Actions Window

---

The Edit Actions window lets you define the threshold values and resulting actions that will be used when MAC-to-IP address binding violations occur on the device.



Thresholds are the number of violations that must occur on a single MAC-to-IP address binding before an action is performed. Each threshold can be assigned one or more of the following actions: sending a syslog message, sending an audit trap, or applying a quarantine policy. If you assign a quarantine action, you must associate a valid quarantine policy with the quarantine action. For more information, refer to [How to Create a Quarantine Role](#).

Up to six thresholds can be configured per port class. Typically, thresholds values are set to a low number. For example, you could configure a threshold value of 2 to trigger a syslog message to alert administrators of a binding violation. You could configure another threshold value of 5 to assign a quarantine role to a user. That way, if a user continues to violate a binding, you can restrict their access until the cause of the violation can be determined.

Access the window from the Device Configuration sub-tab in the [device Anti-Spoofing tab](#). In the Violation Actions section, select a port class tab. In the table, select an action and click the Edit Actions button to open the window.

---

### Related Information

For information on related tasks:

- [How to Configure Anti-Spoofing](#)
- [Device Anti-Spoofing Tab](#)
- [Port Properties - Anti-Spoofing Tab](#)

## Edit Bandwidth Configuration Window

---

This window lets you configure the arbiter mode for the transmit queues associated with the selected class of service. The arbiter mode is the method used to determine the way that traffic in each queue is serviced. It is based on a percentage or weight (called a "slice") given to each queue. For more information on the arbiter mode, see [Transmit Queue Bandwidth Configuration](#).

---

**NOTE:** The Edit Bandwidth Configuration window configures the arbiter mode for the Default transmit queue port group. If you have configured multiple transmit queue port groups, you can use the [Arbiter Mode tab](#) to configure arbiter mode for the additional groups.

---

The Default transmit queue port group may contain multiple port queue types (for example, 4-queue ports and 16-queue ports) depending on the type of devices on your network. Each port type requires separate arbiter mode configuration using the corresponding subtab in the window

---

**NOTE:** The Edit Bandwidth Configuration window will display subtabs for all the port types supported by the devices on your network, regardless of whether the Default port group contains those port types or not.

---

The **Edit Bandwidth Configuration Window** provides four Transmit Queue Arbiter Modes:

- [Strict](#)
  - [Weighted Fair Queuing](#)
  - [Enhanced Transmission Selection](#)
  - [Use Per-Port Type Arbiter Mode](#)
- 

**NOTE:** Arbiter mode is likely to be incompatible with some devices. If this occurs, you will receive Enforce Preview Errors for those devices and arbiter mode will be skipped.

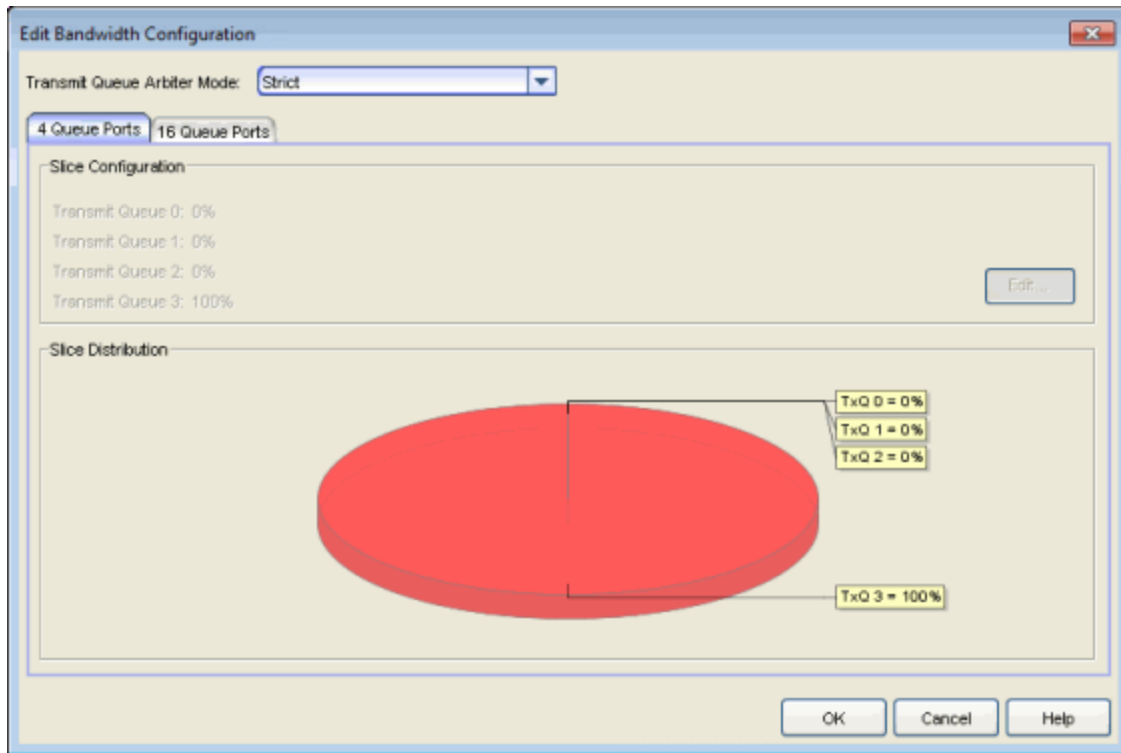
---

### Strict

By default, ports are set to Strict mode, which means that the highest priority queue (the highest numbered queue) is set to 100%. In Strict mode, the highest priority queue (the highest numbered queue) is set to 100%. Queues are serviced by numerical priority from the highest numbered queue to the lowest. Queues

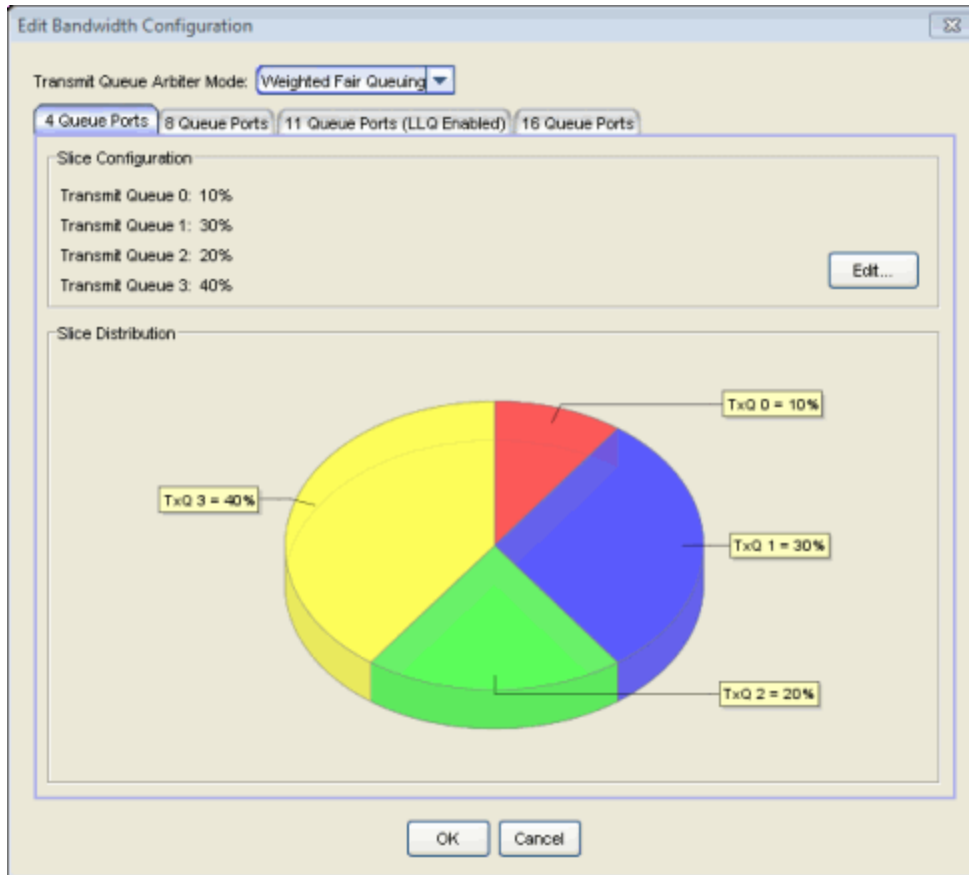


are serviced until empty or until a higher priority queue requires servicing. For example, for a 4-queue port in strict mode, all frames in Transmit Queue 3 will be transmitted before the frames in Transmit Queue 0.



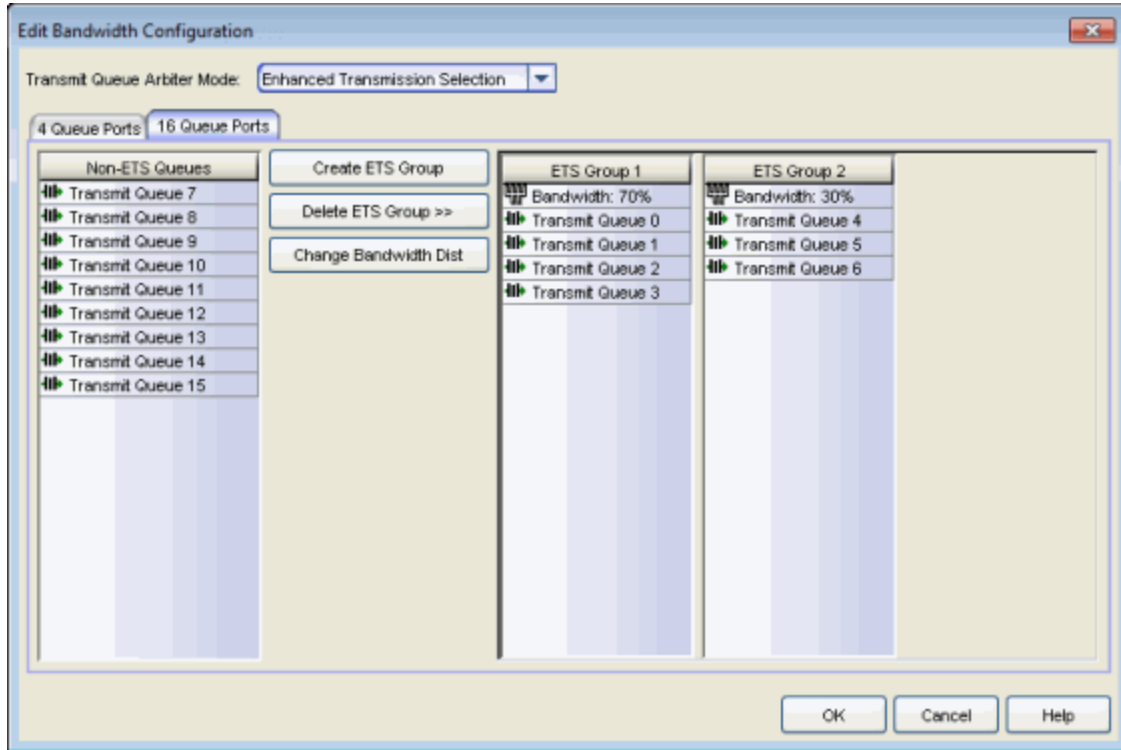
## Weighted Fair Queuing

You can change the arbiter mode to Weighted Fair Queuing, which lets you adjust the slice percentage for each queue, and prevent a lower priority queue from being starved. Queues are serviced according to the percentage or weight you assign to each queue. This prevents a lower priority queue from being starved. Percentages must add up to 100%. Configuring 100% for the highest priority queue sets the port to Strict mode.



## Enhanced Transmission Selection

Allows you to designate 2 or more traffic class queues as ETS queues. Queues can be moved between groups by either right-clicking the queue and selecting the group or dragging and dropping the queue into the group. The ETS queues are then assigned bandwidth allocation with the sum of the ETS queues bandwidth equaling 100%. The scheduler will then service all non-ETS queues first using strict priority. The remaining bandwidth is then distributed based on the allocation that was defined for each of the ETS queues. The priorities within an ETS queue are serviced by strict priority.



### Non-ETS Queues

List of Non-ETS Queues which will be serviced first using strict priority. Queues can be moved by dragging the queue into the desired ETS group, or by right-clicking the queue and selecting the group from the drop-down list.

### Create ETS Group

Click to create a new ETS group. A new group is added to the right pane. By default, bandwidth allocation is set to 100%. Double-click the bandwidth setting to change the allocation value.

### Delete ETS Group >>

Click to select an ETS group to delete. The group is deleted from the right pane.

### Change Bandwidth Dist

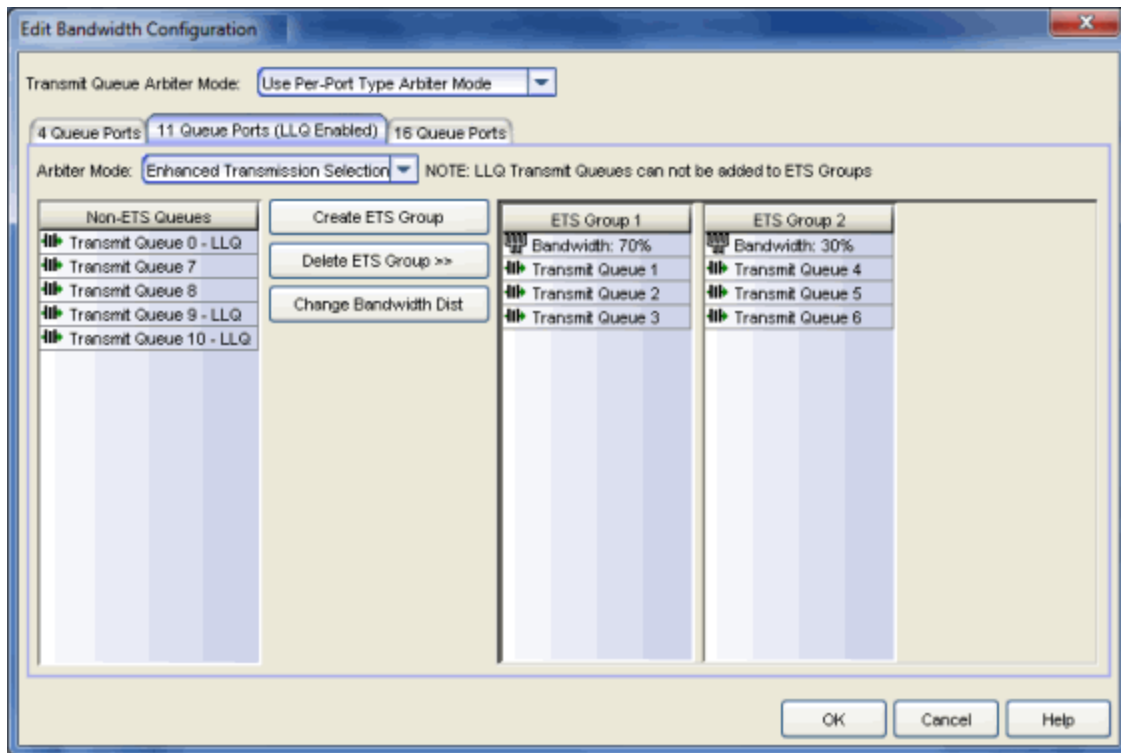
Click to open the Edit Bandwidth dialog. Under Bandwidth Distribution, enter a value for each ETS group. The total of all ETS groups must equal 100%.

### ETS Groups

List of created ETS groups including selected bandwidth allocation and transmit queues.

## Use Per-Port Type Arbiter Mode

Allows you to specify an arbiter mode independently for each port type (for example, 11 Queue Ports or 16 Queue ports).



### Arbiter Mode

Use the drop-down list to select a Transmit Queue Arbiter Mode.

## Slice Configuration

Lists the slice percentages given to each queue on the port. Use the **Edit** button to open the [Edit Slice Percentages window](#) where you can configure the slice distribution for each queue.

## Slice Distribution

Displays the distribution of slice percentages in a graphical format.

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

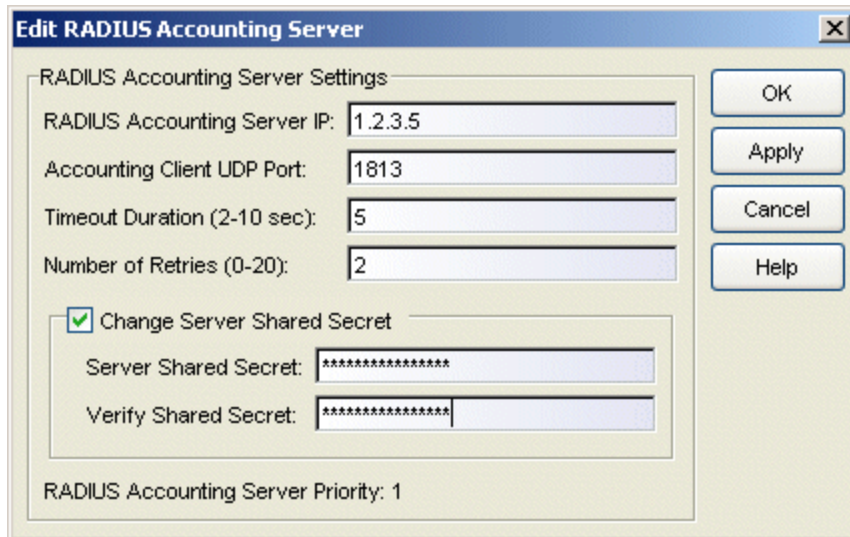
- [How to Configure Transmit Queues](#)

For information on related windows:

- [Edit Slice Percentages Window](#)

## Edit RADIUS Accounting Server Window

Use this window to change the parameters used for communication between a device and a RADIUS accounting server. To access this window, select a server in the RADIUS Server(s) Accounting sub-tab (in the [RADIUS tab](#) for a device), and then click the **Edit** button.



The screenshot shows a dialog box titled "Edit RADIUS Accounting Server". It contains several input fields and a checkbox. The fields are: "RADIUS Accounting Server IP" with the value "1.2.3.5", "Accounting Client UDP Port" with the value "1813", "Timeout Duration (2-10 sec)" with the value "5", and "Number of Retries (0-20)" with the value "2". There is a checkbox labeled "Change Server Shared Secret" which is checked. Below this checkbox are two text boxes: "Server Shared Secret" and "Verify Shared Secret", both containing masked characters (asterisks). At the bottom left, there is a label "RADIUS Accounting Server Priority: 1". On the right side of the dialog, there are four buttons: "OK", "Apply", "Cancel", and "Help".

### RADIUS Accounting Server IP

IP address of the RADIUS accounting server.

### Accounting Client UDP Port

UDP port number (1-65535) the device (RADIUS client) uses to send accounting requests to the RADIUS server; 1813 is the default port number. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Timeout Duration (2 -10 sec)

The amount of time in seconds the device will wait for the RADIUS server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Number of Retries (0-20)

The number of times the device will resend an accounting request if the RADIUS server does not respond. Valid values are 0-20. Devices that do

not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

### Change Server Shared Secret

Check this box to change the string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS server. This shared secret is not to be confused with the RADIUS client/Policy Manager shared secret entered in the Application Shared Secret area of the [RADIUS tab](#).

### Server Shared Secret

Enter the new shared secret. This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above, to verify the change.

### RADIUS Accounting Server Priority

Order in which the RADIUS accounting server will be checked, as compared to the other RADIUS accounting servers on the device. The lower the number, the higher the priority.

---

## Related Information

For information on related windows:

- [RADIUS Tab](#)

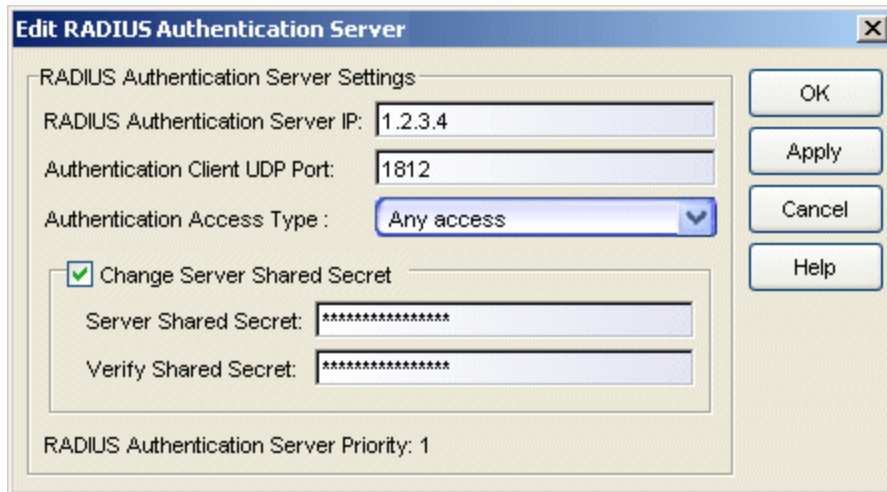
For information on related tasks:

- [How to Configure Devices](#)

## Edit RADIUS Authentication Server Window

---

Use this window to change the parameters used for communication between a device and a RADIUS authentication server. To access this window, select a server in the RADIUS Server(s) Authentication sub-tab (in the [RADIUS tab](#) for a device), and then click the **Edit** button.



### RADIUS Authentication Server IP

IP address of the RADIUS authentication server.

### Authentication Client UDP Port

UDP port number (1-65535) the device (RADIUS client) uses to send authentication requests to the RADIUS server; 1812 is the default port number.

### Authentication Access Type

Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- **Any access** - the server can authenticate users originating from any access type.
- **Management access** - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication. This feature allows you to have one set of servers for authenticating



management access requests and a different set for authenticating network access requests. Devices that do not support this feature will have this field grayed out.

### Change Server Shared Secret

Check this box to change the string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS server. This shared secret is not to be confused with the RADIUS client/Policy Manager shared secret entered in the Application Shared Secret area of the [RADIUS tab](#).

### Server Shared Secret

Enter the new shared secret. This string must match the shared secret entered when you [added the client device](#) on the RADIUS server. Without the shared secret, the server and client will be unable to communicate, and authentication attempts will fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

### Verify Shared Secret

Re-enter the Server Shared Secret you entered above, to verify the change.

### RADIUS Authentication Server Priority

Order in which the RADIUS authentication server will be checked, as compared to the other RADIUS authentication servers on the device. The lower the number, the higher the priority.

---

## Related Information

For information on related concepts:

- [Authentication](#)

For information on related windows:

- [RADIUS Tab](#)

For information on related tasks:

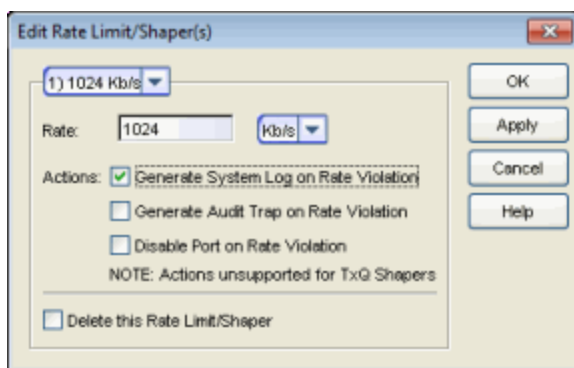
- [How to Configure Devices](#)
- [Authentication Configuration Guide](#)

## Edit Rate Limit/Shaper Window

---

This window lets you edit or delete a rate limit or rate shaper. Rate limits/shapers are components of a Policy Manager class of service, and are used to control the transmit rate at which traffic enters and exits ports in your network.

To access this window, open the [Class of Service Configuration Window](#) (available from the Policy Manager Edit menu). Double-click a rate in the table and select Edit/Delete Rates/Actions from the drop-down menu. You can edit the actual rate and actions, or delete the rate completely.



### Rate Limit

Specify the highest transmission rate at which traffic can enter or exit a port before packets will be rate limited:

- % - A percentage of the total bandwidth available (not available for priority-based rate limits)
- PPS - Packets per second (not available for priority-based rate limits)
- Kb/s - Kilobits per second
- Mb/s - Megabits per second
- Gb/s - Gigabits per second

### Actions

Select the action type(s) you would like this rate limit to use:

- Generate System Log on Rate Violation - a syslog message is generated when the rate limit is first exceeded.
- Generate Audit Trap on Rate Violation - an audit trap is generated when the rate limit is first exceeded.

- Disable Port on Rate Violation - the port is disabled when the rate limit is first exceeded.

---

**NOTE:** N-Series Gold devices do not support rate limit notification.

---

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)
- [How to Define Rate Limits](#)

## Edit Rule Window

---

The Edit Rule window allows you to change the traffic description associated with a rule. The Traffic Description, which includes the traffic classification layer, traffic classification type, and traffic value, was entered when the rule was created (see [How to Create or Modify a Rule](#)).

There are two ways to display the Edit Rule window:

- Select the rule in the left panel's Services tab and the General tab in the right panel. In the Traffic Description section, click **Edit** to bring up the Edit Rule window.
- Select a Manual service in the left panel's Services tab and the Details View tab in the right panel. Double-click the Traf Desc Value column to open the Edit Rule window.

If you modify an enabled rule's traffic descriptions, Policy Manager checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See [Conflict Checking](#) for more information.

The contents of the Edit Rule window varies according to the selected rule and traffic description, and which tab you have accessed the window from.

The screenshot shows the 'Edit Rule' window with the following configuration:

- Layer:** Traffic Classification Layer: All Layers
- Type:** Traffic Classification Type: IP TCP Port Source
- Value:**
  - IP TCP Port Source**
  - Select a TCP type from the choice box below, or choose 'other' and type in a custom one in decimal form. You may also enter a range of values for this Traffic Description. Range rules are not supported on legacy devices.
  - Well-Known Values: FTP Data (20)
  - Other:
    - Single Value: 20
    - Range: Start Value: [ ], End Value: [ ]
  - Enter a valid IP Address in the text box below. (XXX.XXX.XXX.XXXh)
  - Note: The IP Address is an optional field and does not have to be specified. It is only valid for non-range port values.
  - Value: [ ]

## Layer Area

### Traffic Classification Layer

The OSI model classification layer (or All Layers) currently associated with the rule. Each layer has multiple classification types from which you can select. If you change the layer, the Type and Value sections in the window change, and you must make new selections in those sections. See [Classification Types and their Parameters](#) for information.

## Type Area

### Traffic Classification Type

The traffic classification type currently associated with the rule. Each classification type consists of certain parameters and/or values. If you

change the type, the Value section of the window changes, and you must make new selections in that section. See [Classification Types and their Parameters](#) for information.

## Value Area

This area displays the values currently selected for the traffic classification type, and allows you to change those values. Each traffic classification type requires certain parameters and/or values. See [Classification Types and their Parameters](#) for parameter information.

---

### Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)

For information on related windows:

- [General Tab \(Rule\)](#)

## Enforce Preview Window

---

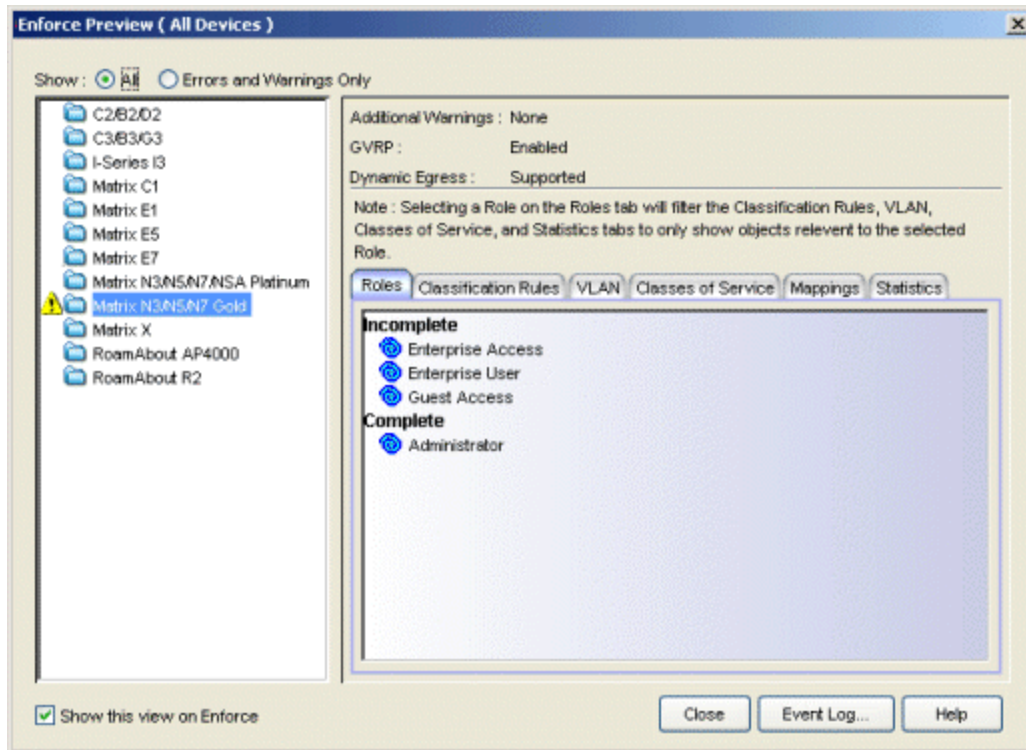
Use the Enforce Preview window to view the information that will be written to your devices, before you actually [enforce](#). This feature is particularly useful if you have devices that only support certain aspects of policy management. For example, some devices support only the policy features of policy management; some devices support the policy features and classification rules, but do not support VLAN forwarding for certain classification rules; and some devices fully support all policy management features, including policy, classification rules, and VLAN forwarding for all classification rules.

The Enforce Preview window appears whenever you click the **Enforce** button, or select the **File > Enforce Role Set** menu option, or double-click the enforce icon on the status bar, so that you always get a chance to review the effects of enforcing prior to actually performing the enforce. You can control whether or not this view automatically appears with the **Show this view on Enforce** checkbox, or in [Optional Views](#) in the Options window.

You can also access this window from the **File > Enforce Preview** menu option, and from the **Enforce Preview** button on the confirmation message that appears when a [verify](#) has taken place.

What you see in the window depends on whether you would be enforcing to all devices or to a subset of devices. The title bar indicates the devices to which the enforce will apply. After viewing the information in this window, you can either click **Cancel** to back out and make fixes, or **Enforce** to go ahead with the enforce. (The **Enforce** button does not appear in this window when you use the **File > Enforce Preview** menu option to launch the window.)

You can view device support for specific [roles](#), [services](#), and [rules](#) on their Device Support tabs. Refer to the NetSight Firmware Support tables for complete information on device support for Policy Manager features, and VLAN and Priority classification rules.



## "Show" Radio Buttons

What you see in the right panel of the Enforce Preview window depends on which radio button you have selected at the top of the window.


### All

Select this radio button to display what will *and* what will not be written to the devices when you enforce.

### Errors and Warnings Only

Select this radio button to show only what will *not* be written to the devices when you enforce.

## Left Panel

The left panel of the Enforce Preview window displays folders for different device types. Expand the folders to see your network devices and device groups organized according to device type. The  icon alerts you that there are certain things that will not be written to this device type that you might want to investigate prior to enforcing (e.g. rules that are not supported on a device).



Select a specific device type to display the information that will be written to those devices when you enforce.

### Show this view on Enforce

When this checkbox is checked, the Enforce Preview window will appear any time you [enforce](#), before the actual enforcement takes place. You can also turn this option on and off via [Optional Views](#) in the Options window.

## Right Panel

The upper portion of the right panel provides information about whether certain policy management features are supported and/or enabled for the device type selected in the left panel.

- Additional Warnings - If there are additional problems detected with the enforce, you will be directed to see the Event Log for details.
- GVRP - Shows whether GVRP is Enabled, Disabled, or Ignored. You can change GVRP status for the domain via the Edit menu.
- Dynamic Egress - Shows whether [Dynamic Egress](#) is Supported or Not Supported.

There are six tabs that provide specific information about the Roles, Classification Rules, VLANs, Classes of Service, and Mappings that will be enforced. The information displayed depends on the device type you've selected in the left panel, and whether you have the [Show All](#) or the [Show Errors and Warnings Only](#) radio button selected. In addition, select a role in the Roles tab to filter the information for just that role.

### Roles Tab

**Incomplete** - Lists any roles with unsupported classification rules. These roles will be written to the devices, but without the unsupported rules.

**Complete** - Lists any roles which do *not* include unsupported classification rules. These roles will be written to the devices as defined.

---

**NOTE:** Select a Role to display only those classification rules and VLANs associated with the selected role.

---

### Classification Rules Tab

**Excluded** - Lists any unsupported classification rules that have been applied to a role. These rules will not be included when the associated roles are written to the devices.

**Included** - Lists any supported classification rules that have been applied to

a role. These rules will be included when the associated roles are written to the devices.

---

**NOTE:** On N-Series Platinum devices, range classification rules are achieved through applying subnet masks to values. As such, in order to achieve a user-specified range, the device may need multiple rules with subnets applied to encompass that range. So, although the user created only one rule with a range, this list may show multiple instances of that rule with the name of the rule followed by the portion of the over-all range it applies to.

---

### VLAN Tab

**Excluded** - Lists any VLANs associated with unsupported classification rules, or VLANs that are not supported by the device. These VLANs will not be written to the devices.

**Included** - Lists any VLANs associated with supported classification rules and VLANs associated with roles. These will be written to the devices.

### Classes of Service Tab

**Class of Service Mode** - Lists the Class of Service mode that will be written to the devices.

**Classes of Service Subtab** - Lists the classes of service that will be written to the devices:

- Class of Service - the name of the class of service.
- 802.1p Priority - the priority associated with the class of service.
- ToS Value - the IP type of service value associated with this class of service, if any. See [IP Type of Service](#) for more information.
- Drop Prec - The drop precedence associated with this class of service, if any. See [Drop Precedence](#) for more information.
- TxQueue Index - the transmit queue index associated with the class of service.
- IRL Index - the role-based inbound rate limit index associated with the class of service.
- ORL Index - the role-based outbound rate limit index associated with the class of service.

For more information, see [Getting Started with Class of Service](#) and [How to Create a Class of Service](#).

**Inbound/Outbound Role-Based Rate Limit Mappings Subtabs** - Lists the rate limit mappings that will be written to the devices:

- Device - The device where the rate limit mapping will be in effect.
- IRL/URL Port Grp - The name of the port group that contains the rate limit mapping.
- IRL/URL Index - The logical inbound rate limit (IRL) or outbound rate limit (URL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming packets.
- Rate Limit - The actual rate limit that the IRL/URL index is mapped to.
- IRL/URL Port Type - The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).
- Information - Information about mapping support.

**Transmit Queue/Rate Shaper Mappings Subtab** - Lists the transmit queue rate shaper mappings that will be written to the devices:

- Device - The device where the transmit queue rate shaper mapping will be in effect.
- TxQ Port Grp - The name of the port group that contains the transmit queue rate shaper mapping.
- TxQ Index - The logical transmit queue rate shaper index number. This index number is specified in a class of service and dictates the transmit queue and rate shaper behavior for incoming packets.
- Physical Transmit Queue / Rate Shaper - The actual transmit queue rate shaper that the index is mapped to.
- TxQ Port Type - The type of ports included in the port group. Port type is based on the number of transmit queues the ports support (for example, 4-transmit queue ports and 16-transmit queue ports).
- Information - Information about mapping support.

## Mappings Tab

---

**WARNING:** Enforcing port-level MAC to Role mappings could potentially remove rules created by NetSight Automated Security Manager (ASM) as an intrusion detection response.

---

**MAC to Role Mapping** - Lists the device-level and port-level mappings that will be written to the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- MAC Address - the MAC address mapped to the role. Masking a MAC address is only supported on N-Series Platinum devices.
- Mask - the mask associated with the MAC address.
- Role - the role mapped to the MAC address.

**IP to Role Mapping** - Lists the device-level mappings that will be written to the devices:

- IP Address - the IP address mapped to the role.
- Mask - the mask associated with each IP address. Masking an IP address is only supported on N-Series Gold and Platinum devices.
- Role - the role mapped to the IP address.

**Tagged Packet VLAN to Role Mapping** - Lists the device-level and port-level mappings that will be written to the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

**Authentication Based VLAN (RFC 3580) to Role Mapping** - Lists the mappings that will be written to the devices:

- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

## Statistics Tab

**Device Statistics** - Lists role count information about each device. If the number of roles in the domain exceeds the supported number of roles on a device, then enforce will fail.

- Supported # of Roles - The maximum number of roles supported by the device.
- Domain Role Count Supported - This column says "No" if the number of roles in the domain exceeds the supported number of roles on the device. A "Yes" in this column indicates that the number of roles on

the device is equal to or less than the maximum number of supported roles.

**Role Statistics** - Lists information about each role:

- Number of Rules - The number of traffic classification rules the role includes.
- Number of Unique Masks - The number of masks defined for the rules included in the role.

### Enforce Button

[Enforces](#) the roles, classification rules and VLANs in the current data file to the devices, based on the level of support available on the devices as indicated in the Enforce Preview window. This button does not appear in this window when you use the **File > Enforce Preview** menu option to launch the window.

---

### Related Information

For information on related concepts:

- [Enforcing](#)

For information on related windows:

- [Device Support Tab \(Role\)](#)
- [Device Support Tab \(Rule\)](#)
- [Device Support Tab \(Service\)](#)

## Event Details Window

---

The Event Details window shows information about a single event selected in the Event Log. To access the window, right-click an event in the Event Log and select **Event Details** from the menu.

The screenshot shows the 'Event Details' window with the following fields and values:

Timestamp:	09/27/2005 09:34:38 AM	Acknowledged:	No
Type:	Event	Source:	---
Event Name:	Client Startup	Client:	cardent-XP2
Severity:	Info	User:	CTRON/cardent
Category:	Application		
Information:	Client Startup		
Enterprise:		Trap Number:	
Description:	<div style="border: 1px solid black; height: 150px; width: 100%;"></div>		

Buttons at the bottom: OK, Acknowledge, Help

### Timestamp

The date and time when the event occurred.

### Acknowledged

Whether or not the selected event has been acknowledged.

### Type

The type of information: Event.

**Source**

The IP address of the host that was the source of the event.

**Event Name**

The type of event.

**Client**

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

**Severity**

The event's severity.

**Category**

The category of event.

**User**

The name of the user that triggered the event.

**Information**

Information about the event.

**Enterprise**

Not applicable to the Policy Manager Event Log.

**Trap Number**

Not applicable to the Policy Manager Event Log.

**Description**

Not applicable to the Policy Manager Event Log.

**OK Button**

Closes the window.

**Acknowledge/Unacknowledge Button**

Places a check or removes a check in the Acknowledge column in the Event Log for the selected event.

---

**Related Information**

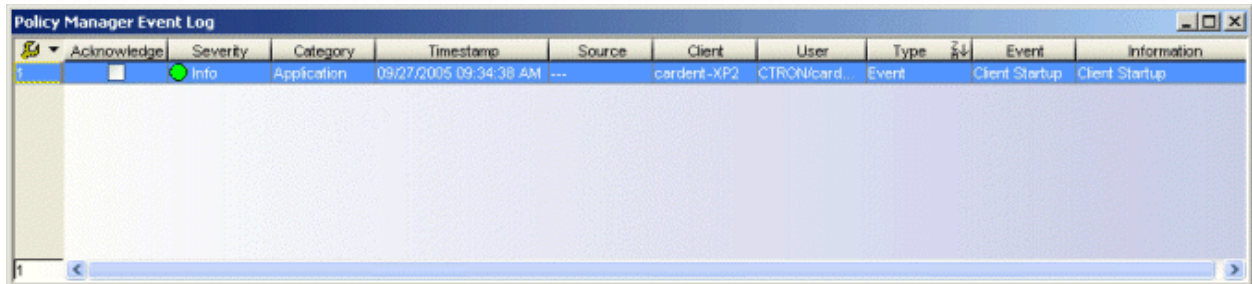
For information on related windows:

- [Event Log](#)

## Event Log

---

Access the Event Log by clicking the Events button in the Policy Manager toolbar. The Event Log displays error and informational messages about Policy Manager system operations.



The screenshot shows the 'Policy Manager Event Log' window. It features a table with the following columns: Acknowledge, Severity, Category, Timestamp, Source, Client, User, Type, Event, and Information. A single event is listed with the following details:

Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event	Information
<input type="checkbox"/>	Info	Application	09/27/2005 09:34:38 AM	---	cardent-XP2	CTRON\card...	Event	Client Startup	Client Startup

### Acknowledge

This checkbox lets you acknowledge an event.

### 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.



## Right-Click Menu Options

The event log right-click menu lets you *Acknowledge* and *Unacknowledge* events. 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:

- [Event Details Window](#)


## Filter Window

---

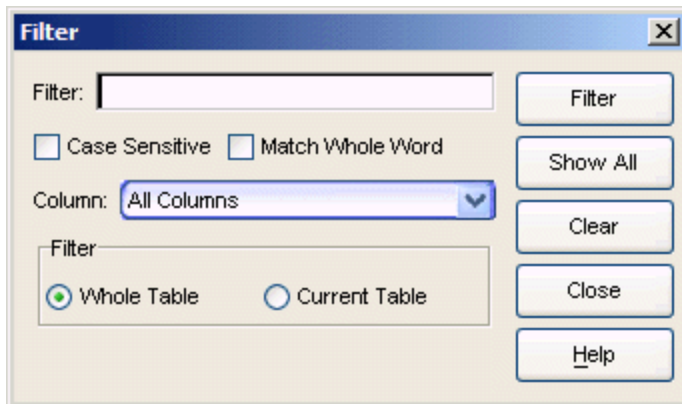
The Filter window lets you specify which entries to display in the right panel. When the information in the right panel is presented in a column format, you can perform a filter, and only those entries matching your filter criteria will be displayed. You can filter the entries in a single column or in all columns, and you can apply consecutive filters.

You can access the Filter window by selecting **View > Filter**. You can also right-click on a column header and select **Filter**.

---

**NOTE:** Some Policy Manager tables use a set of Table Tools to find, filter, sort, print, and export information in a table. You can access these Table Tools by clicking the Table Tools  button in the upper left corner of the table. For more information, see Table Tools.

---



### Filter

Enter the numeric value or text you want to filter.

### Case Sensitive

Select the **Case Sensitive** check box to filter based on the exact case of the text entered in the **Filter** field.

### Match Whole Word

Select the **Match Whole Word** check box to filter based on the entire text or numeric value entered in the **Filter** field.

### Column

Use the **Column** drop-down list to select the column you want to filter. Select **All Columns** to filter all entries.

**Whole Table**

Select the **Whole Table** option to filter all entries by the value in the **Filter** field. If you have already performed a filter, this will enable you to perform a new filter on all entries instead of just the filtered entries.

**Current Table**

Select the **Current Table** option to perform a new filter on the results of the previous filter.

**Filter Button**

Click **Filter** to perform the filter operation.

**Show All Button**

Click **Show All** to remove any filters and display all entries.

**Clear Button**

Click **Clear** to clear the information entered in the **Filter** field.

**Close Button**

Click **Close** to exit the Filter window.

---

**Related Information**

For information on related tasks:

- [How to Filter, Find, and Sort](#)


## Find Window

---

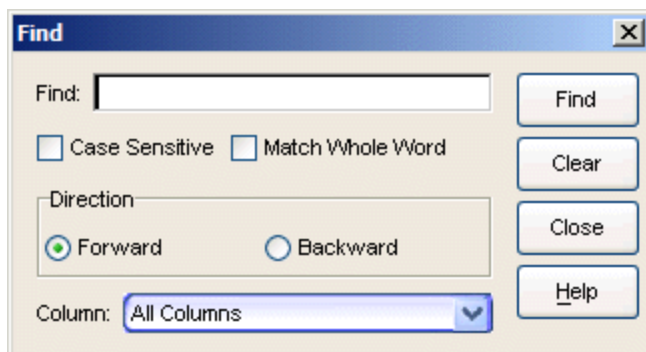
The Find window lets you search the right panel for a specific text or value. When the information in the right panel is presented in a column format, you can perform a find, and the entry that matches the search criteria is highlighted in the right panel. You can search in a single column or in all columns. You can also search forward or backward from your current position, and restrict your search to match the exact case and/or whole word of the entry.

You can access the Find window by selecting **Edit > Find**. You can also right-click on a column header and select **Find**.

---

**NOTE:** Some Policy Manager tables use a set of Table Tools to find, filter, sort, print, and export information in a table. You can access these Table Tools by clicking the Table Tools  button in the upper left corner of the table. For more information, see Table Tools.

---



### Find

Enter the value you are searching for.

### Case Sensitive

Select the **Case Sensitive** check box to search based on the exact case of the text entered in the **Find** field.

### Match Whole Word

Select the **Match Whole Word** check box to search based on the entire text or numeric value entered in the **Find** field.

### Forward

Select **Forward** to search from your current position to the end of the table.

**Backward**

Select **Backward** to search from your current position to the beginning of the table.

**Column**

Use the **Column** drop-down list to select the column you want to search. Select **All Columns** to search all entries.

**Find Button**

Click **Find** to search based on the value in the **Find** field and the parameters selected.

**Clear Button**

Click **Clear** to clear the information entered in the **Find** field.

**Close Button**

Click **Close** to exit the Find window.

---

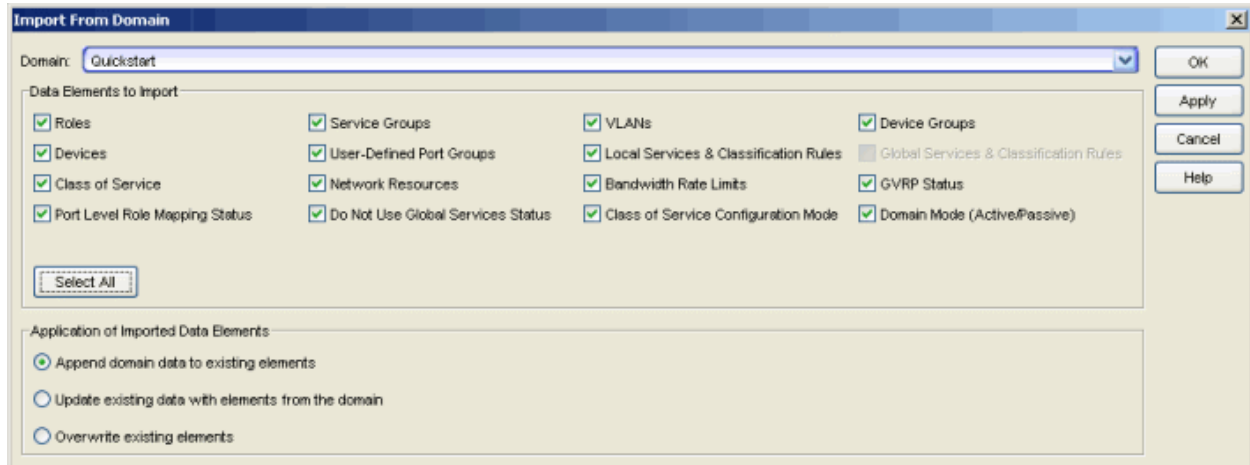
**Related Information**

For information on related tasks:

- [How to Filter, Find, and Sort](#)

## Import from Domain Window

This window lets you import policy configuration data from one [Policy Domain](#) into another domain. To access the Import from Domain window, select **File > Import > Import From Domain**. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)



### Domain

Use the drop-down list to select the domain whose data you want to import.

## Data Elements to Import

In this section, you can choose the specific data elements you want to import. Click **Select All** to select all the data import options at once.

### Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist in the current domain, or if you are importing them at the same time as the role, the services will be associated with the role. Otherwise, the services will not be imported.

### Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services will be associated with the group. Otherwise, the services will not be imported.

## VLANs

Select this option to import VLANs.

### Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

## Device Groups

Select this option to import device group names. If you are importing a device group's devices at the same time as the device group, the devices will be associated with the device group. Otherwise, the devices will not be imported.

## Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the NetSight database or they won't be imported. (See [How to Add and Delete Devices](#) for more information on using Console to add devices to the NetSight database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy Manager Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

## User-Defined Port Groups

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports will be associated with the port group. Otherwise, the ports will not be imported.

### Local Services and Classification Rules

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, Policy Manager checks for rule conflicts (see [Conflict Checking](#) for more information).

### Global Services and Classification Rules

Since Global services are common to all domains, this option does not apply when importing from a domain.

### Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to [import rate limits](#), the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired. Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See [append](#), [update](#) and [overwrite](#) for information on how those specific actions affect the import of classes of service.

### Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the [General tab](#) for the service.

### Bandwidth Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. When you [append](#) or [update](#) rate limits and a duplicate rate limit exists in the current domain, any unique priority and exclusion properties of the imported rate limit replace (if appending) or are added to (if updating) those of the first duplicate rate limit in the existing [precedence](#) list. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an



existing rate limit, it will not be imported. If you also elect to [import classes of service](#), the rate limits are imported first, then the classes of service are imported. See [append](#) and [update](#) for information on how those specific actions affect the import of rate limits.

**Note:** Only those network elements that are recognized by the existing domain can be imported as exclusions. Others will be ignored.

### **GVRP Status**

Select this option to import the GVRP status for the domain (as specified in the Edit menu).

### **Port-Level Role Mapping Status**

Select this option to import the [Port-Level Role Mappings Enabled](#) status for the domain, as specified in the Edit menu.

### **Do Not Use Global Services Status**

Select this option to import the Do Not Use Global Services status for the domain, as specified in the Edit menu.

### **Class of Service Configuration Mode**

Select this option to import the class of service mode (basic or advanced) for the domain, as specified in the Edit menu.

### **Domain Mode**

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

## **Application of Imported Data Elements**

In this section, you can choose how you want the data elements selected above to update your current domain.

### **Append domain data to existing elements**

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be changed.

**Rate Limits:** A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

**CoS:** A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but

the rate limits for the imported class of service do not match the existing rate limit settings.

#### Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

**Rate Limits:** A rate limit will not be updated if the rate limit and direction do not match.

**CoS:** A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

#### Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

**CoS:** A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.

---

**NOTE:** If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

---

#### Select All Button

Selects all of the data elements.

#### OK Button

Imports the selected data and closes the window.

#### Apply Button

Imports the selected data and leaves the window open.

---

### Related Information

For information on related tasks:

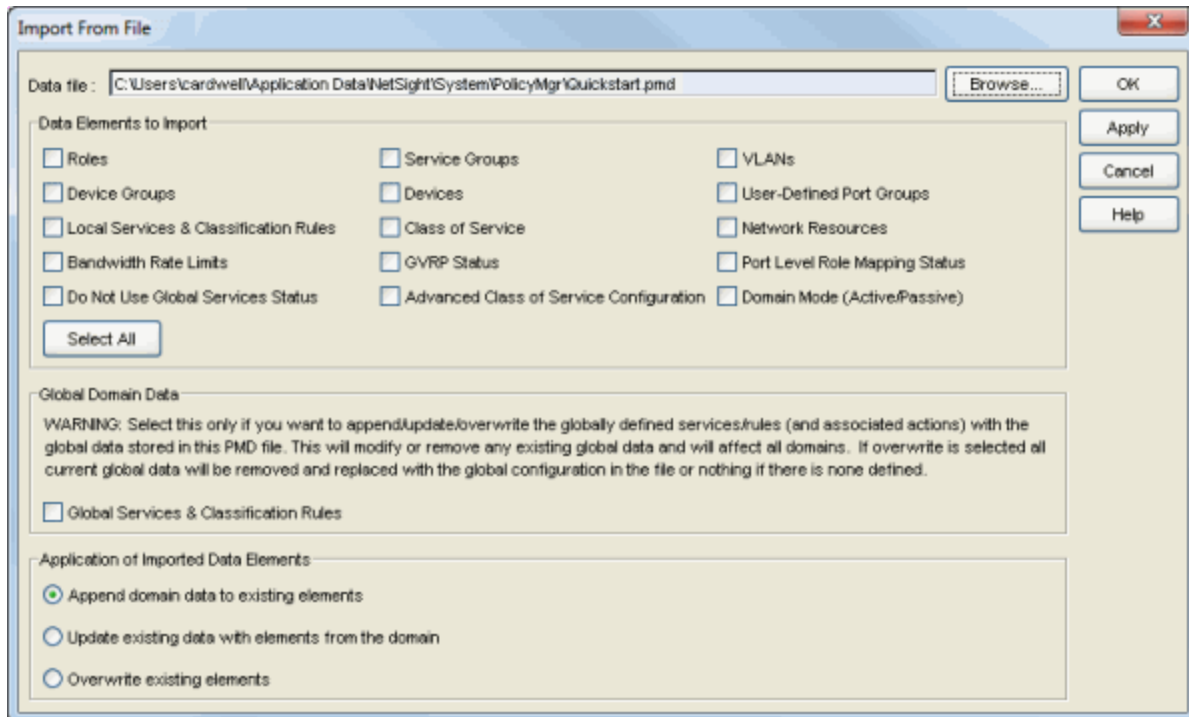
- [How to Create and Use Domains](#)
- [How to Import From Device](#)

For information on related windows:

- [Import From File Window](#)

## Import from File Window

This window lets you import policy data from a .pmd file or .xml file into a Policy Domain. To access the window, select **File > Import > Import From File**.



### Data file

Enter the name and path for the data file (.pmd or .xml) you want to import, or navigate to the file.

### Data Elements to Import

In this section, you can choose the specific data elements you want to import. Click **Select All** to select all the data import options at once.

### Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist in the current domain, or if you are importing them at the same time as the role, the services will be associated with the role. Otherwise, the services will not be imported.

### Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services will be associated with the group. Otherwise, the services will not be imported.

### VLANs

Select this option to import VLANs.

#### Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

### Device Groups

Select this option to import device group names. If you are importing a device group's devices at the same time as the device group, the devices will be associated with the device group. Otherwise, the devices will not be imported.

### Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the NetSight database or they won't be imported. (See [How to Add and Delete Devices](#) for more information on using Console to add devices to the NetSight database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy Manager Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to

the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

### User-Defined Port Groups

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports will be associated with the port group. Otherwise, the ports will not be imported.

### Local Services and Classification Rules

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, Policy Manager checks for rule conflicts (see [Conflict Checking](#) for more information).

### Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to [import rate limits](#), the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired. Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See [append](#), [update](#) and [overwrite](#) for information on how those specific actions affect the import of classes of service.

### Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the [General tab](#) for the service.

### Bandwidth Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. When you [append](#) or [update](#) rate limits and a duplicate rate limit exists in the current domain, any unique priority and exclusion properties of the

imported rate limit replace (if appending) or are added to (if updating) those of the first duplicate rate limit in the existing [precedence](#) list. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an existing rate limit, it will not be imported. If you also elect to [import classes of service](#), the rate limits are imported first, then the classes of service are imported. See [append](#) and [update](#) for information on how those specific actions affect the import of rate limits.

**Note:** Only those network elements that are recognized by the existing domain can be imported as exclusions. Others will be ignored.

### GVRP Status

Select this option to import the GVRP status for the domain (as specified in the Edit menu).

### Port-Level Role Mapping Status

Select this option to import the [Port-Level Role Mappings Enabled](#) status for the domain (as specified in the Edit menu).

### Do Not Use Global Services Status

Select this option to import the Do Not Use Global Services status for the domain, as specified in the Edit menu.

### Advanced Class of Service Configuration

Select this option to import the class of service configuration (basic or advanced) for the domain, as specified in the Edit menu (whether the Advanced Class of Service Configuration option is selected).

### Domain Mode

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

## Global Domain Data

Use this option only if you want to append, update, or overwrite the globally defined services and rules in your current domain with the global domain data stored in the .pmd file you are importing. This option will modify or remove any existing global data and will affect all domains. If overwrite is selected, all current global data will be removed and replaced with the global configuration in the file, or nothing if there is no configuration defined.

### Global Services and Classification Rules

Select this option to import Global services (services that are common to all domains) and their associated classification rules. When you import rules from another domain, Policy Manager checks for rule conflicts (see [Conflict Checking](#) for more information).

## Application of Imported Data Elements

In this section, you can choose how you want the data elements selected above to update your current domain.

### Append domain data to existing elements

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be changed.

**Rate Limits:** A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

**CoS:** A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but the rate limits for the imported class of service do not match the existing rate limit settings.

### Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

**Rate Limits:** A rate limit will not be updated if the rate limit and direction do not match.

**CoS:** A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

### Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

**CoS:** A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.



**NOTE:** If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

---

**Select All Button**

Selects all of the data elements.

**OK Button**

Imports the selected data and closes the window.

**Apply Button**

Imports the selected data and leaves the window open.

---

**Related Information**

For information on related tasks:

- [How to Create and Use Domains](#)
- [How to Import From Device](#)

For information on related windows:

- [Import From Domain Window](#)

## Main Window

---

The Policy Manager main window is the central point for all Policy Manager tasks. It is divided into a left panel and a right panel. The tabs in the left panel display hierarchical trees that represent the roles, services, network elements, and port groups involved in managing policies for your network. The tabbed pages in the right panel display detailed information about the item selected in the left panel.

The trees in the left panel tabs can be organized in different "tab configurations." By default, Policy Manager opens using a Consolidated Tab Configuration. In the Consolidated Tab Configuration, there are two left-panel tabs: Roles/Services and Network Elements/Port Groups. Access Control, Class of Service, and Network Resources are launched in separate configuration windows from the Edit menu.

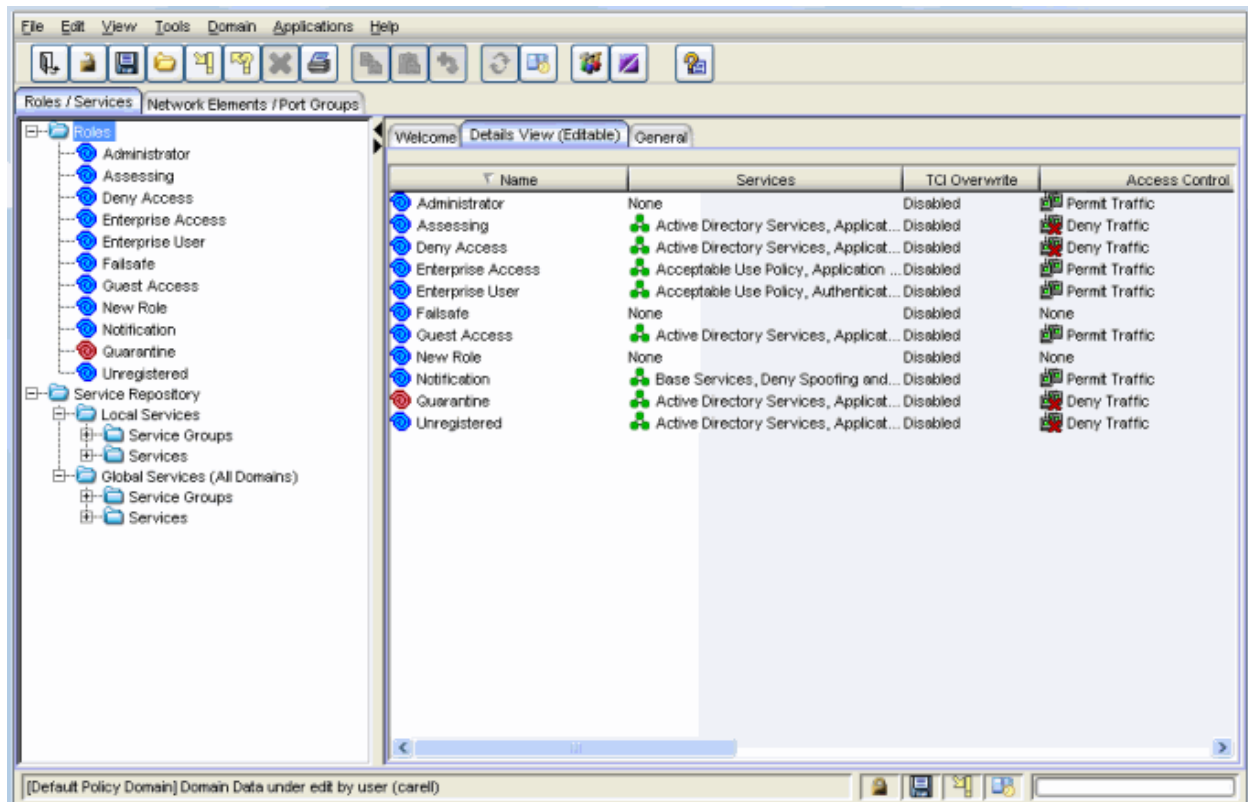
You can change the tab configuration using the Tab Configuration option panel (Tools > Options > Tab Configuration), if desired. Instead of the Consolidated Tab Configuration, you can select the Classic Tab Configuration which was used in Policy Manager prior to version 4.0, or a Custom Tab Configuration which allows you to define which tab the different trees will be organized under. Whatever configuration you select in the options panel will be the default configuration used by all domains. However, you can also override the default configuration on a per-domain basis using the View > Domain Tab Configuration menu. For more information on available Tab Configurations, see the [Tab Configuration Option](#) Help topic.

The menu bar and the toolbar at the top of the window provide access to Policy Manager functions and let you perform policy-related tasks. The status bar at the bottom of the window displays error and status information.

### Information on the Main window features:

- [Dialog Boxes \(Messages\)](#)
- [Icons](#)
- [Left Panel](#)
- [Menu Bar](#)
- [Right Panel](#)

- [Status Bar](#)
- [Toolbar](#)































## Dialog Boxes (Messages)

In the course of using Policy Manager, you will see message dialog boxes confirming that certain tasks have been completed, or warning you of the consequences of a certain action. Many of these dialog boxes give you the option of turning off subsequent displays of the message, and once you have become accustomed to using Policy Manager you may want to take advantage of this option. You can also turn off the display of *all* information message dialog boxes in the [Dialog Boxes view](#) accessible from the **Tools > Options** menu option. In that view, you can also turn on the message dialog boxes that you have turned off on the individual dialog box(es).

## Icons

The icons used in Policy Manager and their meanings are as follows:

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

## Status Bar Icons

The following icons appear in the status bar:



### Lock

Reminds you that the current Policy Domain is locked for editing purposes. You can lock and unlock the domain from the Lock tool bar button.



### Save

Reminds you that you've made changes, and that you need to save the Policy Manager data to the Policy Domain. Double-clicking this icon initiates the save operation. Only users with the capability to Enforce will be able to save the domain.



### Enforce

Reminds you that you've made changes to roles that you need to enforce. Double-clicking this icon initiates the enforce operation.



### Event Log

This icon is displayed when a new Warning or Error message has been logged to the Event Log. Double-click the icon to open the [Event Log](#).

[window.](#)

---

## Related Information

For information on related windows:

- [Details View Tabs](#)
- [Dialog Boxes View](#)
- [Left Panel](#)
- [Menu Bar](#)
- [Right Panel](#)
- [Status Bar](#)
- [Toolbar](#)

## Left Panel

---

The left panel of the Policy Manager main window contains tabs that display hierarchical trees representing the roles, services, network elements, and port groups involved in managing policies for your network. What you select in the left panel determines what is displayed in the right panel.

The trees in the left panel tabs can be organized in different "tab configurations." By default, Policy Manager opens using a Consolidated Tab Configuration. In the Consolidated Tab Configuration, there are two left-panel tabs: Roles/Services and Network Elements/Port Groups. Access Control, Class of Service, and Network Resources are launched in separate configuration windows from the Edit menu.

You can change the tab configuration using the Tab Configuration option panel (Tools > Options > Tab Configuration), if desired. Instead of the Consolidated Tab Configuration, you can select the Classic Tab Configuration which was used in Policy Manager prior to version 4.0, or a Custom Tab Configuration which allows you to define which tab the different trees will be organized under. Whatever configuration you select in the options panel will be the default configuration used by all domains. However, you can also override the default configuration on a per-domain basis using the View > Domain Tab Configuration menu. For more information on available Tab Configurations, see the [Tab Configuration Option](#) Help topic.

When you first open Policy Manager, the Roles tab is displayed in the left panel, by default. The [Select Tree at Startup option](#) (Tools > Options > Tab Configuration) lets you select any of the other left-panel tabs to be displayed in subsequent startups. There is also an option to display the same tab you were using when you last closed Policy Manager.

Features of the left panel include:

- *Expanding and collapsing items in the hierarchy:* Double-click the item or its icon, or single-click the turner to the left of the icon.
- *Right-click menus:* Right-click a folder or other item in the left panel, and a menu of the options you can perform on your selection appears.
- *Drag and drop:* Populate port groups, services, and service groups by using drag and drop in the left panel. You can also drag and drop multiple selections from right-panel Details View tab lists in the Services tab.

**Information on the left-panel tabs:**

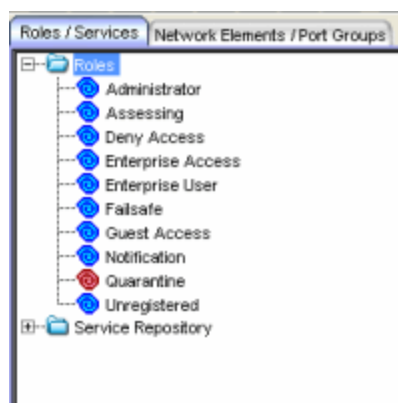
- [Roles/Services Tab](#)
- [Network Elements/Port Groups Tab](#)
- [Access Control Configuration](#)
- [Class of Service Configuration](#)
- [Network Resources Configuration](#)

## *Roles/Services Tab*

This tab displays the Roles and Service Repository trees.

### Roles Tree


The Roles tree lists the roles defined for the current domain. A [role](#) is a set of network access services that can be applied at various access points in a policy-enabled network.



### Roles Folder

This folder contains the roles defined for the current domain. See [How to Create a Role](#) for more information.

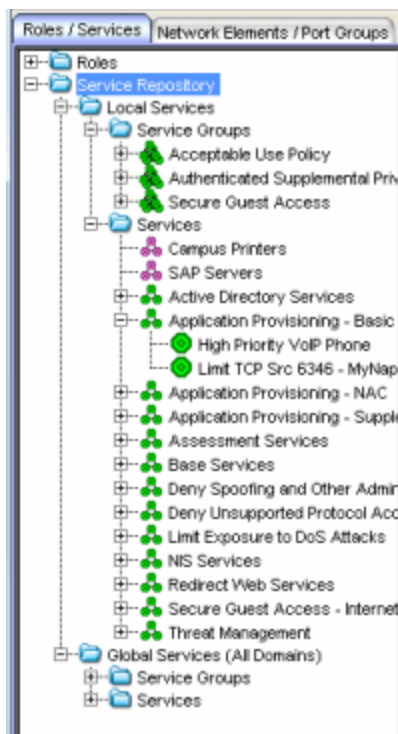
### Role

Individual roles are listed by name. Select a role in the left panel, and view information about that role in the right-panel tabs. Only [Quarantine roles](#) are displayed with a red icon .

### Service Repository Tree

The Service Repository tree displays your Local and Global services and service groups. [Services](#) are sets of rules that define how network traffic for a particular network service or application should be handled by a network access device. Local Services are services that are unique to the current domain. Global Services

are services that are common to all domains. The tab also displays your [network resource groups](#).



### Local Services Folder

Local Services are services that are unique to the current domain. This folder contains the local service groups and services defined for the current domain. For more information, see [How to Create a Service Group](#).

### Global Services Folder

Global Services are services that are common across all domains. This folder contains the global service groups and services that are shared by all domains. For more information, see [How to Create a Service Group](#).

### Service Groups Folder

Policy Manager lets you create categories (service groups) into which you can group services. This folder contains the service groups that have been defined. For more information, see [How to Create a Service Group](#).

### Service Group

Individual service groups are listed by name. Expand the service group to see the services and service groups included in that group.



## Services Folder

This folder contains the automated and manual services that have been defined. For more information, see [How to Create a Service](#).

## Automated Service

Individual [Automated services](#) are listed under the Services Folder or within a service group in the Service Groups folder.



## Manual Services Folder

This folder contains your currently defined [Manual services](#).

## Manual Service

Individual [Manual services](#) are listed under the Services Folder. Expand the service to see the rules associated with it.

## Rule

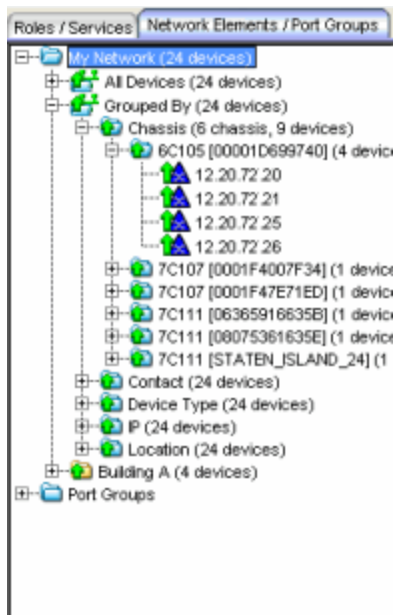
Individual rules are listed by name. If the rule is disabled, the rule icon displays a red X . If the rule is device-specific, the rule icon displays a small switch .

## *Network Elements/Port Groups Tab*

This tab displays the My Network and Port Groups trees.

## My Network Tree

The My Network tree displays the devices that are assigned to the current domain, organized into groups.



## My Network

My Network displays the system-created device groups and any user-created device groups (that you created through NetSight Console). Each device group name is followed by the total number of devices in that group and any subgroups, in parentheses.

## All Devices Folder

This folder contains all the devices that are assigned to the current domain. For information on adding devices to the domain, see [How to Add and Delete Devices](#).

## Grouped By Folder

The top-level Grouped By folder contains five system-created groups: Chassis, Contact, Device Type, IP, and Location. When a device is assigned to a domain, it automatically becomes a member of the appropriate group. System-created groups are displayed with blue folders.

## Chassis Folder

Contains subgroups for specific chassis in the domain.

## Contact Folder

Contains subgroups of the devices in a domain based on the system contact. Sub-groups in this folder are automatically created based on the Contact value in the Console Properties (Device) tab. For example, a contact defined as *NOC/Salem/Jones* will automatically create a hierarchy of three sub-groups under the **Grouped By > Contact** folder. The Contact sub-groups are removed when the last device with a particular contact is deleted.

## Device Type Folder

Contains subgroups for the specific product families and device types in the domain.

## IP Folder

Contains subgroups based on the IP subnets in the domain.

## Location Folder

Contains subgroups of the devices in a domain based on the system location. Sub-groups in this folder are automatically created based on the Location value in the Console Properties (Device) tab. For example, a location defined as *NewHampshire/Salem/Closet1* will automatically create a hierarchy of three sub-groups under the **Grouped By > Location** folder. The Location sub-groups are removed when the last device for a particular location is deleted.

## User-created Device Groups

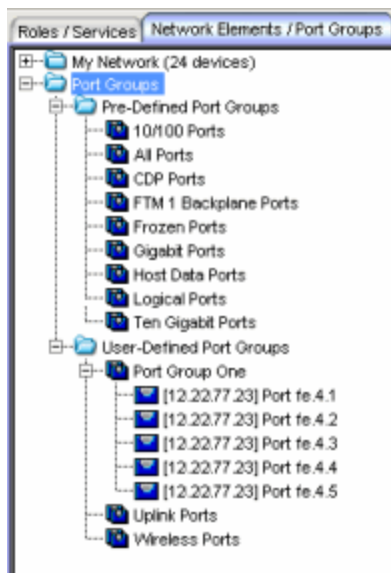
You can add your own device groups and subgroups (displayed with yellow folders) using NetSight Console.

## Device

This icon represents an individual device that has been assigned to the current domain. It appears below the Devices folder and also below any device group of which it is a member.

## Port Groups Tree

This tree displays the pre-defined and user-defined [port groups](#) for the current domain.



## Port Groups Folder

This folder contains the Pre-Defined and User-Defined Port Groups for the current domain. Policy Manager allows ports to be combined into groups, similar to the way devices are combined into device groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. For more information, see [How to Create a Port Group](#).

## Pre-Defined Port Groups Folder

Policy Manager provides you with several commonly used port groups for your convenience. Expand this folder to see the pre-defined port groups. For more information, see [Pre-Defined Port Groups](#).

### User-Defined Port Groups Folder

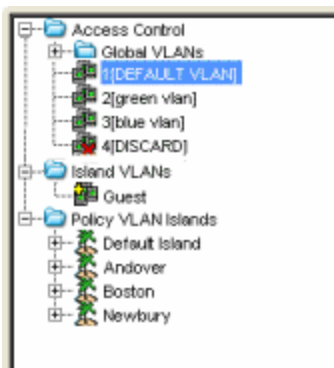
Policy Manager lets you create your own port groups. When you create a user-defined port group, you can select individual ports to add to the group.

### Port Group

Select a port group in the left panel and view information about that group in the right-panel tabs.

## Access Control Configuration


The left panel tree in the Access Control Configuration window (available from the Policy Manager Edit menu) displays the Global VLANs for the current domain. If you have enabled Policy VLAN Islands, it also displays your Island VLANs and [Policy VLAN Islands](#).



### Global VLANs Folder

This folder contains your currently defined [global VLANs](#) for this domain.

### VLAN

The VLAN icon indicates the access control for the VLAN-- if it is a Discard VLAN, the icon displays a red X . Otherwise, it is a Contain VLAN.

### Island VLANs Folder

This folder appears only when the [Policy VLAN Islands](#) feature is enabled, and contains your currently defined [Island VLANs](#) for this domain.

### Policy VLAN Islands Folder

This folder appears only when the [Policy VLAN Islands](#) feature is enabled, and contains your currently defined VLAN islands and the devices that belong to them. When you enable Policy VLAN Islands, this folder is pre-populated with a Default Island containing all the devices in the domain.

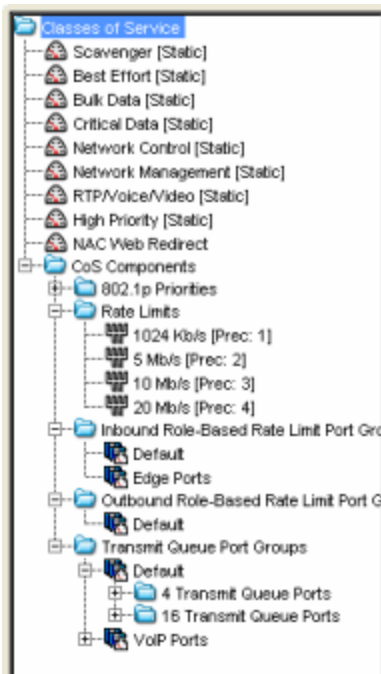
## VLAN Island 🌳

Click on a [VLAN island](#) to see the devices associated with it listed in the right-panel Details View tab. The Default Island is created by Policy Manager when you enable Policy VLAN Islands, and it cannot be deleted.

## Class of Service Configuration

The left panel tree in the Class of Service Configuration window (available from the Policy Manager Edit menu) displays your Classes of Service defined for the current domain. The tree is only displayed when you are in Advanced Mode.

Classes of Service prioritize traffic with an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an Automated service, or as a role default. For more information, see [Getting Started with Class of Service](#).



## Classes of Service Folder

When you first install Policy Manager, the left-panel Classes of Service folder is pre-populated with eight classes of service, each associated with one of the 802.1p priorities (0-7). These are static classes of service and cannot be deleted. You can use these classes of service as is, or configure them to include ToS/DSCP, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own

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

### Class of Service

Select a Class of Service in the left panel, and view information about that service in the right-panel tabs. For more information, see [How to Create a Class of Service](#).

### CoS Components Folder

This folder contains subfolders of the possible components of a class of service (802.1p Priorities, Rate Limits, Role-Based Rate Limit Port Groups, and Transmit Queue Port Groups).

### 802.1p Priorities Folder

This folder contains the eight 802.1p priorities. Select a priority in the left panel, and view information about that priority in the right-panel tabs.

### Rate Limits Folder

This folder contains the currently defined rate limits, listed in the order of precedence. For more information, see [How to Define Rate Limits](#).

### Rate Limit Port Groups

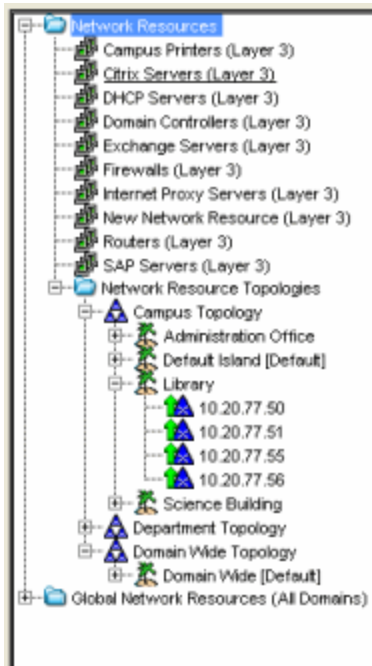
These folders contain the currently defined inbound and outbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see [Creating Class of Service Port Groups](#).

### Transmit Queue Port Groups Folder

This folder contains the currently defined transmit queue port groups and the transmit queues defined for each group. For more information, see [How to Configure Transmit Queues](#).

## *Network Resources Configuration*

The left panel tab in the Network Resource Configuration window (available from the Policy Manager Edit menu) displays the network resources and network resource topologies for the current domain.



### Network Resources Folder

This folder contains any [network resource groups](#) you have created. For more information, see [How to Create a Network Resource](#).

### Network Resource

Individual network resource groups are listed by name. Select a resource in the left panel, and view information about that resource in the right-panel tabs.

### Network Resource Topologies Folder

This folder contains the [network resource topologies](#) currently defined for this domain.

### Network Resource Topology

A network resource topology can be used to divide the devices in a domain into groups called islands. You can then define a unique network resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate. If you are not using custom topologies to group your devices, you will use the Domain Wide topology, which contains just one island for all your domain devices.

### Topology Island

A topology island is a group of devices that have a unique network resource list, allowing you to set up network resource access based on the

location where end users authenticate.

### Global Network Resources Folder

Global Network Resources are network resources that are common across all domains. For more information, see [How to Create a Network Resource](#).

---

### Related Information

For information on related windows:

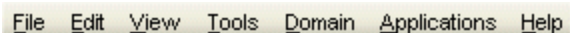
- [Main Window](#)
- [Right Panel](#)



## Policy Manager Menus

---

The menu bar on the Main Window provides access to Policy Manager functions. Some sub-items on the menu are standard, and some depend on what left-panel item and right-panel tab you have selected. When you have something specific selected in the left or right panel (e.g., a device, service, VLAN), it may be more convenient to use the right-click menu for the selection, instead of the menu bar. For information on menu options available only from right-click menus, see [Right-click Menu Options](#).



File Edit View Tools Domain Applications Help

### *File Menu*

The File Menu provides file management options for Policy Manager.

#### **File > Lock Policy Domain**

Lets you lock the current Policy Domain for editing purposes. Policy Manager automatically locks the domain when you begin to edit the domain configuration. Other Policy Manager clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released. For more information, see [Controlling Client Interactions with Locks](#). This menu option serves the same function as the **Lock** button on the toolbar.

#### **File > Save Policy Domain**

Lets you save any changes you have made to the current Policy Domain. Only users with the capability to Enforce will be able to save the domain. This menu option serves the same function as the **Save** button on the toolbar.

#### **File > Read Policy Domain**

Lets you update the current Policy Domain with the latest saved domain data. This menu option serves the same function as the **Read** button on the toolbar.

#### **File > Export to File**

Lets you save policy data from the current Policy Domain to a .pmd file or .xml file with the file name and location of your choosing. This file stores all information about roles, services, and rules configured in the current Policy Domain. This allows you to save a Domain configuration prior to making

changes so that you can restore the original Domain configuration if required (via File > Import> Import From File).

#### **File > Import > Import From Domain**

Opens the [Import from Domain window](#) where you can import policy configuration data from one Policy Domain into another domain. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)

#### **File > Import > Import From File**

Enables you to import policy data from a .pmd file into the current Policy Domain. Be aware that the import overwrites any existing data in the Policy Domain. Any devices in the .pmd file must already exist in the Console database or they won't be imported.

#### **File > Import > Policy Configuration From Device**

Enables you to import policy configurations (roles and rules) from a selected device or devices into your Policy Domain.

#### **File > Enforce Role Set**

Writes the role and/or any changes you have made to it (rules, services) to all the devices in your current domain. You have a chance to review the effects of enforcing on the [Enforce Preview window](#), if it is enabled. This menu option serves the same function as the **Enforce (Global)** button on the toolbar. See [Enforcing](#) for more information.

#### **File > Enforce Preview**

Opens the [Enforce Preview window](#), where you can view the effects of [enforcing](#) prior to the actual enforcement.

#### **File > Verify Role Set**

Compares the roles in your current domain to the roles currently enforced on all the devices in the current domain. This is useful for ensuring that the roles in your domain have been enforced, or, if you use more than one domain, ensuring that the roles in the domain you are currently using matches what is on the devices. This menu option serves the same function as the **Verify (Global)** button on the toolbar. See [Verifying](#) for more information.

#### **File > Database > Initialize Database Components**

Provides a way for you to initialize only the Policy Manager components in the NetSight Database.

**File > Delete**

Deletes the current selection in the left panel. This menu option serves the same function as the **Delete** button on the toolbar.

**File > Print**

Opens a platform-dependent print setup window for printing the contents of the currently displayed selection in the right panel in text format. This menu option serves the same function as the **Print** button on the toolbar.

**File > Exit**

Exits the Policy Manager application. If there is unsaved or unenforced data, you will be asked if you wish to update the database and/or enforce before exiting. This menu option serves the same function as the **Exit** button on the toolbar.

*Edit Menu*

The Edit Menu options change depending on what is currently displayed in the left and right panels.

**Edit > Copy**

Copies an item selected in the left panel or right panel. This menu option serves the same function as the **Copy** button on the toolbar.

**Edit > Paste**

Pastes what has been copied into the specified location. This menu option serves the same function as the **Paste** button on the toolbar.

**Edit > Add**

Adds or applies what has been copied to the currently selected item. This menu option serves the same function as the **Add** button on the toolbar.

**Edit > Find**

Lets you search the currently displayed right panel tab for specified criteria.

**Edit > Clear Disabled Ports (Rule Hits)**

Clears any ports that have been disabled due to a "rule hit" and re-enables them. For more information, see the [Rule Usage tab](#).

**Edit > Rename**

Lets you edit the name of the currently selected item. Some of the elements that come pre-packaged with Policy Manager cannot be renamed (e.g., Pre-Defined Port Groups).

**Edit > Add/Remove Ports**

Lets you add and remove ports from the selected user-defined port group.

**Edit > Add/Remove Services**

Lets you add and remove services from the selected service group.

**Edit > Pre-Defined Well-Known IDs**

Opens the [Pre-Defined Well-Known IDs window](#), where you can add to the pre-defined list of well-known identifiers (IDs) used when creating Policy Manager rules.

**Edit > Access Control Configuration**

Opens the Access Control Configuration window where you can configure parameters for the VLANs defined in your network. You can also configure Policy VLAN Islands if you select the Policy VLAN Islands Enabled option in the Edit menu.

**Edit > Class of Service Configuration**

Opens the Class of Service Configuration window where you can configure the [Classes of Service](#) defined in your network.

**Edit > Network Resources Configuration**

Opens the Network Resource Configuration window where you can configure the [network resources](#) and [network resource topologies](#) for your network.

**Edit > GVRP > Ignore GVRP**

To ignore GVRP status on the devices in the current domain, select this menu option and [enforce](#). This means that Policy Manager will ignore the GVRP configuration on a device during an Enforce operation, allowing you to configure some network devices with GVRP enabled and others with GVRP disabled (using MIB Tools or local management), according to their configuration requirements. Be aware that for devices with GVRP set to disabled, ignoring GVRP configuration during an Enforce may affect connectivity on ports with VLANs that rely on Dynamic Egress.

**Edit > GVRP > Enable GVRP**

To enable GVRP on the devices in the current domain, select this menu option and [enforce](#). If the current domain configuration contains rules that use VLAN containment, Dynamic Egress and GVRP must be enabled on the devices in the domain, or the VLANs must be properly pre-configured on the devices outside of Policy Manager.

**Edit > GVRP > Disable GVRP**

If you do not want GVRP enabled on the devices in the current domain, select this menu option and [enforce](#). Be aware that disabling GVRP may affect connectivity through ports with VLANs that rely on Dynamic Egress.

**Edit > Passive Domain Mode**

Check this box to enable [Passive Domain Mode](#) for the current domain.

**Edit > Policy VLAN Islands Enabled**

Check this box to enable [Policy VLAN Islands](#) for the current domain.

**Edit > Port Level Role Mappings Enabled**

Check this box to enable any port-level Tagged Packet VLAN to role mappings or port-level MAC to role mappings that have been configured and enforced for the current domain. If the box is not checked, all port-level mappings are ignored.

**Edit > Do Not Use Global Services**

Check this box to hide the display of Global Services in the left-panel Services tab for this domain. If you use Global Services in some domains but not in others, this option allows you to hide global services in the domains where they are not used so that they won't be inadvertently used or modified.

**Edit > Delete**

Deletes the current selection in the left panel. This menu option serves the same function as the **Delete** button on the toolbar.

*View Menu*

Lets you make changes to the appearance of the Policy Manager main window and the information contained in the right panel. The View Menu options depend on what is currently selected in the left panel.

**View > Tool Bar**

Lets you hide or display the Tool Bar by selecting or deselecting the check box.

**View > Status Bar**

Lets you hide or display the Status Bar by selecting or deselecting the check box.

**View > Sort**

Opens the Sort window, which lets you sort the information in the right panel in ascending or descending order by column. For instructions, see

---

### [Sorting](#).

**View > Filter**

Opens the Filter window, which allows you to select specific information to display in the right panel. For instructions, see [Filtering](#).

**View > Refresh**

Updates the contents of the right panel. This can be useful for rereading device information after downloading new firmware or for refreshing port authentication information. This menu option serves the same function as the Refresh button on the toolbar.

**View > Policy Classification Rules**

Opens the [Policy Classification Rules window](#), where you can view all of the Policy Manager rules that exist in the currently active domain, along with information about each rule.

**View > CoS Usage**

Opens the [Classes of Service Usage window](#), where you can view information about current class of service usage on a port.

**View > Event Log**

Opens the [Event Log](#) window, where you can view error and informational messages about Policy Manager system operation. This menu option serves the same function as the Event Log button on the toolbar.

**View > Policy Rule Hit**

[Policy Rule Hit Reporting](#) provides a historical look at rule usage over time for domains. When rule accounting is enabled on a device, the Policy Rule Hit data is collected through syslog messages sent from the device to the NetSight server and stored in the NetSight database. This information is displayed in the various Policy Rule Hit Reports accessed from this menu option.

**View > Domain Tab Configuration**

Opens the [Domain Tab Configuration window](#) where you can override the default tab configuration and specify a custom tab configuration for the current domain that is open.

### *Tools Menu*

Lets you perform administrative tasks on roles, services, devices, and VLANs. The Tools Menu options vary depending on what is currently selected in the left panel or right panel. The options are listed alphabetically, so their placement on the actual menu may differ from the listing here.

**Tools > Add/Remove Ports**

Opens the [Add/Remove Ports window](#), where you can add and remove ports to and from role-based rate limit port groups and transmit queue port groups.

**Tools > Add to Role(s)**

With a service or service group selected, opens the Add to Role window where you can select the roles to which you want to add the services.

**Tools > Assign Devices to Domain**

Opens the [Assign Devices to Domain window](#) where you can assign devices that are in the NetSight database to the current Policy Domain.

**Tools > 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.

**Tools > Classification Rule Wizard**

Starts the Rule Wizard, a series of windows that leads you through all the steps required to create a new traffic classification rule. For instructions, see [Using the Rule Wizard](#).

**Tools > Clear Frozen**

With a device selected, unfreezes all the ports on the selected device. With one or more ports selected, unfreezes the port(s). See [How to Freeze/Unfreeze a Port](#) for more information.

**Tools > Create Classification Rule**

Creates a "New Rule" item in the left panel's Services tab, which you can then change to the desired rule name. Use this option if you want to create a traffic classification rule without using the Rule Wizard. For instructions, see [Using the Rule Tabs](#).

**Tools > Create Class of Service**

Opens the [Create Class of Service window](#), where you can define a new class of service. See [How to Create a Class of Service](#) for more information.

**Tools > Create Policy VLAN Island**

Expands the [Policy VLAN Islands](#) folder in the left-panel VLANs tab, and creates a "New Island" item, which you can then change to the desired VLAN island name. At the same time, the right panel displays the Details View for the new VLAN island. While you can use this option to create an VLAN island, it is recommended you use the [Policy VLAN Islands](#)

---

[Configuration Wizard](#) to lead you through the creation and configuration of VLAN islands.

**Tools > Create Port Group**

Expands the User-Defined Port Groups folder in the left panel's Port Groups tab, and creates a "New Port Group" item, which you can then change to the desired port group name. For instructions, see [How to Create a Port Group](#).

**Tools > Create Role**

Creates a "New Role" item in the left panel's Role tab, which you can then change to the desired role name. Use this function when you want to create a role without using the Role Wizard. For instructions, see [Using the Role Tabs](#).

**Tools > Create Service**

Creates a "New Service" item in the left panel's Services tab, which you can then change to the desired service name. Use this option if you want to create a service without using the Service Wizard. For instructions, see [Using the Service Tabs](#).

**Tools > Create Service Group**

Expands the Service Groups folder in the left panel's Services tab, and creates a "New Service Group" item, which you can then change to the desired service group name. For instructions, see [Creating a Service Group](#).

**Tools > Create VLAN**

Opens the [Create VLAN window](#). For instructions, see [How to Create a VLAN](#).

**Tools > Device Configuration Wizard**

Starts the Device Configuration Wizard, a series of windows that lets you define an authentication configuration and a RADIUS configuration, then apply it to the devices of your choosing. For instructions, see [Using the Device Configuration Wizard](#).

**Tools > Disable Rule(s)**

This menu option disables a single-selected rule, multi-selected rules in the right panel, or all the rules for a selected service (Manual services only).

**Tools > Enable Rule(s)**

This menu option enables a single-selected rule, multi-selected rules in the right panel, or all the rules for a selected service (Manual services only).



**Tools > Export Service(s) to File**

Lets you save one or more service or service groups to a services.pmd file (Policy Manager Database file).

**Tools > MIB Tools**

Opens MIB Tools that allows you to navigate the supported MIBs, examine MIB objects and perform SNMP sets to change their value.

**Tools > Move to Global Services**

Lets you move one or more local services to the Global Service folder.

**Tools > Move to Local Services**

Lets you move one or more global services to the Local Service folder.

**Tools > Options**

Opens the Options window where you can set suite-wide options and [Policy Manager options](#).

**Tools > Policy VLAN Islands Configuration Wizard**

Starts the [Policy VLAN Islands Configuration Wizard](#), a series of windows that helps you create and configure [Policy VLAN Islands](#), as well as select the devices that will comprise each island.

**Tools > Port Configuration Wizard**

Starts the Port Configuration Wizard, a series of windows that leads you through all the steps required to configure a port, including setting the authentication status, login settings, and default role. For instructions, see [Using the Port Configuration Wizard](#).

**Tools > Properties**

Opens the [Port Properties window](#) where you can view general information about the selected port, and also view and change various port configuration settings.

**Tools > Reload VLAN**

Rereads the VLAN settings on your devices and refreshes the list of VLANs in the left-panel VLANs tab.

**Tools > Remove Device(s) from Group**

Removes the device currently selected in the left-panel Network Elements tab from the user-defined device group.

**Tools > Remove Port(s) from Group**

Removes the port currently selected in the left-panel Port Groups tab from the user-defined port group.

**Tools > Remove Service(s) from Group**

Removes the services currently selected in the left-panel Services tab from the service group.

**Tools > Role Wizard**

Starts the Role Wizard, a series of windows that leads you through all the steps required to create a role. For instructions, see [Creating a Role Using the Role Wizard](#).

**Tools > Save Service(s) As**

Enables you to save the selected service(s) to a Policy Manager data (.pmd) file. Special characters such as / \ : ? " < > | are not allowed in the file name. The service name is not case-sensitive; therefore, Policy Manager sees X.pmd and x.pmd as the same service name.

**Tools > 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.

**Tools > Service Wizard**

Starts the Service Wizard, a series of windows that leads you through all the steps required to create a service. For instructions, see [Using the Service Wizard](#).

**Tools > Set Default Role**

Opens the Roles Selection View, where you can assign a [default role](#) to a selected device or device group in the left-panel Network Elements tab. For instructions, see [Assigning Default Roles to Ports](#).

**Tools > Set Frozen**

With a device selected, freezes all the ports on the selected device. With one or more ports selected, freezes the port(s). See [How to Freeze/Unfreeze a Port](#) for more information.

**Tools > Terminate Session(s)**

Terminates the user's session on the selected port(s). If multiple ports are selected, only authenticated sessions whose Terminate Cause is "Not Applicable" are affected. You cannot terminate sessions on frozen ports. See [Terminating a Session](#) for more information.

*Domain Menu*

Lets you create, rename, and delete Policy Domains, and assign devices to the current domain. The bottom part of the menu displays all of your domains and

lets you switch between multiple domains.

#### **Domain > Assign Devices to Domain**

Opens the [Assign Devices to Domain window](#) where you can assign devices that are in the NetSight database to the current Policy Domain.

#### **Domain > Find Domain By IP Address**

Opens the Find Domain By IP Address window that lets you quickly locate the domain where a specific device is assigned. This window is useful when you need to locate a device among multiple domains. Enter an IP address and click **Find**. The window displays the domain where the device is located and allows you to open the domain, if desired. If a device is not assigned to a domain, "Unassigned" is displayed.

#### **Domain > Create Domain**

Lets you create and name a new (blank) Policy Domain.

#### **Domain > Rename Domain**

Lets you rename the current Policy Domain.

#### **Domain > Delete Domain(s)**

Opens a window where you can select one or more Policy Domains to delete.

#### **Domain > Create Mixed-Stack C2/C3/B2/B3 Domain**

Opens a window where you can manage mixed stacks of C2/C3 and B2/B3 devices by creating a new domain specifically for those mixed stack devices, using the data in the currently active domain.

#### **Domain > Show All Rules for All Domains**

Opens the [Policy Classification Rules window](#), where you can view all of the Policy Manager rules that exist in all your domains, along with information about each rule.

#### **Domain > Generate Policy Report**

Use this menu option to automatically generate a summary report of the current domain's policy configuration in PDF format. The report is saved to the following directory: Documents and Settings\`<user home directory>`\Application Data\NetSight\System\PolicyMgr. Each report contains a description of the domain, plus a detailed summary of each of the domain's roles and services, and the rules contained in each service. In addition, the report provides information on the devices assigned to the domain, the domain's Network Resources, Class of Service information (including transmit queues and rate limiting information), and VLAN information.

### *Applications Menu*

Lets you launch other installed NetSight applications from Policy Manager.

### *Help Menu*

Lets you access the components of the Policy Manager online information system.

#### **Help > Topics**

Opens the Policy Manager Help system.

#### **Help > Release Notes**

Displays the NetSight Policy Manager Release Notes for the current release.

#### **Help > About This Window**

Displays detailed information about the currently selected right-panel tab or window. This menu option serves the same function as the **Help** button on the toolbar.

#### **Help > 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.

#### **Help > Support Center**

Opens the Extreme Networks Support website.

#### **Help > Check for Updates**

Allows you to update Policy Manager with the latest version of release notes, new data templates to update the [demo.pmd](#) file, and additions to the pre-defined list of [well-known identifiers \(IDs\)](#). For more information, see Setting Web Update Options.

#### **Help > Getting Started**

Displays the Getting Started help topic that provides an overview of Policy Manager features and functionality. It also includes a summary of the basic steps you must perform to create and configure policies with Policy Manager.

#### **Help > About NetSight Policy Manager**

Displays the NetSight Policy Manager version and copyright information.

### *Right-click Menu Options*

The following menu options are only available from right-click menus. They are listed in alphabetical order.

#### **SSH**

Launches the Secure Shell (SSH) server and, after entering an appropriate username, opens a shell window, which provides the means to communicate with the selected device using a secure command-line based mechanism.

#### **Telnet**

Launches a Telnet session to the selected device's Local Management.

---

### **Related Information**

For information on related windows:

- [Main Window](#)

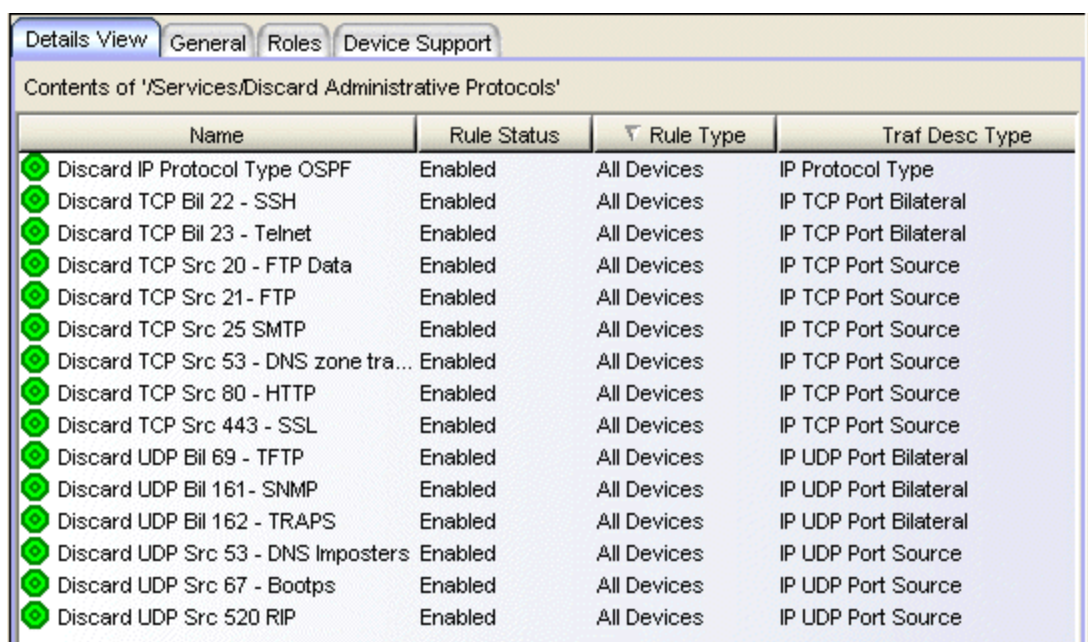
## Right Panel

---

The right panel of the Policy Manager main window displays tabs containing information about the item selected in the left panel.

For some of the items you select in the Policy Manager left panel, the default display in the right panel is a [Details View tab](#). For information on right panel tabs, click on the desired tab under the [Right-Panel Tabs section](#) of the Policy Manager Help Contents panel.

The illustration below shows an example of the Details View tab when you have a service selected in the left panel Services tab.



The screenshot shows a window titled 'Contents of /Services/Discard Administrative Protocols'. It has four tabs: 'Details View' (selected), 'General', 'Roles', and 'Device Support'. Below the tabs is a table with the following columns: Name, Rule Status, Rule Type, and Traf Desc Type. The table lists 15 entries, each with a green status icon, a name, 'Enabled' status, 'All Devices' rule type, and a traffic description type.

Name	Rule Status	Rule Type	Traf Desc Type
Discard IP Protocol Type OSPF	Enabled	All Devices	IP Protocol Type
Discard TCP Bil 22 - SSH	Enabled	All Devices	IP TCP Port Bilateral
Discard TCP Bil 23 - Telnet	Enabled	All Devices	IP TCP Port Bilateral
Discard TCP Src 20 - FTP Data	Enabled	All Devices	IP TCP Port Source
Discard TCP Src 21 - FTP	Enabled	All Devices	IP TCP Port Source
Discard TCP Src 25 SMTP	Enabled	All Devices	IP TCP Port Source
Discard TCP Src 53 - DNS zone tra...	Enabled	All Devices	IP TCP Port Source
Discard TCP Src 80 - HTTP	Enabled	All Devices	IP TCP Port Source
Discard TCP Src 443 - SSL	Enabled	All Devices	IP TCP Port Source
Discard UDP Bil 69 - TFTP	Enabled	All Devices	IP UDP Port Bilateral
Discard UDP Bil 161 - SNMP	Enabled	All Devices	IP UDP Port Bilateral
Discard UDP Bil 162 - TRAPS	Enabled	All Devices	IP UDP Port Bilateral
Discard UDP Src 53 - DNS Imposters	Enabled	All Devices	IP UDP Port Source
Discard UDP Src 67 - Bootps	Enabled	All Devices	IP UDP Port Source
Discard UDP Src 520 RIP	Enabled	All Devices	IP UDP Port Source

---

## Related Information

For information on related windows:

- [Details View Tabs](#)
- [Left Panel](#)
- [Main Window](#)

## Status Bar

---

The status bar at the bottom of the window displays useful information regarding the status of Policy Manager operations. On the left side, the status bar displays the name of the domain that you are currently working in. On the right side, a progress bar shows the percentage of completion for certain lengthy operations. In addition, status bar icons serve as reminders of tasks that need to be performed.



### Lock Icon

Reminds you that the current Policy Domain is locked for editing purposes. You can lock and unlock the domain from the Lock tool bar button.

### Save Icon

Reminds you that you've made changes, and that you need to save the Policy Manager data to the Policy Domain. Double-clicking this icon initiates the save operation. Only users with the capability to Enforce will be able to save the domain.

### Enforce Icon

An Enforce icon is displayed when you have made changes that require you to write the information to your devices. Double-click the icon to perform the enforce operation. For more information, see [Enforcing](#).

### Event Log Icon

An Event Log icon is displayed when a new Warning or Error message has been logged to the Event Log. Double-click the icon to open the [Event Log window](#).

---

## Related Information

For information on related windows:

- [Main Window](#)

## Toolbar

---

The toolbar on the main window provides easy access to some of the more commonly used Policy Manager functions. Some toolbar buttons may not be available, depending on your current location within the Policy Manager application.

You can detach the toolbar from the main window by clicking it and dragging it off the window. To re-attach the toolbar, close the detached toolbar.



### Exit

Closes the Policy Manager application. If there is unsaved or unenforced data, you will be asked if you wish to save domain data and/or enforce before closing. This button serves the same function as the **File > Exit** menu option.

### Lock/Unlock

Lock or unlock the current Policy Domain for editing purposes. Policy Manager automatically locks the domain when you begin to edit the domain configuration. Other Policy Manager clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released. For more information, see [Controlling Client Interactions with Locks](#). This button serves the same function as the **File > Lock/Unlock Policy Domain** menu option.

### Save

Saves any changes you have made to the current Policy Domain. Only users with the capability to Enforce will be able to save the domain. This button serves the same function as the **File > Save Policy Domain** menu option.

### Read

Updates the current Policy Domain with the latest saved domain data. This button serves the same function as the **File > Read Policy Domain** menu option.

### Enforce (Global)

Writes the role and/or any changes you have made to it (rules, services) to all the devices in your current domain. You have a chance to review the effects of enforcing in the [Enforce Preview window](#), if it is enabled. This



button serves the same function as the **File > Enforce Role Set** menu option. See [Enforcing](#) for more information.

### Verify (Global)

Compares the roles in your current domain to the roles currently enforced on all the devices in the current domain. This is useful for ensuring that the roles in the domain have been enforced, or that the roles in the domain match what is on the devices. This button serves the same function as the **File > Verify Role Set** menu option. See [Verifying](#) for more information.

### Print

Prints the contents of the currently displayed right panel. This button serves the same function as the **File > Print** menu option.

### Copy

Copies an item selected in the left panel 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 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.

### Add

Adds or applies what has been copied to the currently selected node. 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 > Add** menu option.

### Delete

Deletes the current selection in the left panel. This button serves the same function as the **File > Delete** menu option.

### Refresh

Updates the contents of the right panel. This can be useful for rereading device information or for refreshing port authentication information. This button serves the same function as the **View > Refresh** menu option.

### Event Log

Opens the Event Log window, where you can view and filter Policy Manager events. This button serves the same function as the **View > Event Log** menu option.

**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.

**Help**

Displays detailed information about the currently selected right-panel tab or window. 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](#)

## Policy Manager Options Window

---

These options apply only to the Policy Manager 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 Policy Manager folder to view all the different options you can set.

Information on the following Options views:

- [Default Class of Service](#)
- [Dialog Boxes](#)
- [Name Resolution \(PM\)](#)
- [Optional Views](#)
- [Policy Rule Hit Reporting](#)
- [Ports](#)
- [Startup](#)
- [SNMP Options](#)
- [Tab Configuration](#)
- [Welcome View](#)
- [Wireshark](#)

### Default Class of Service

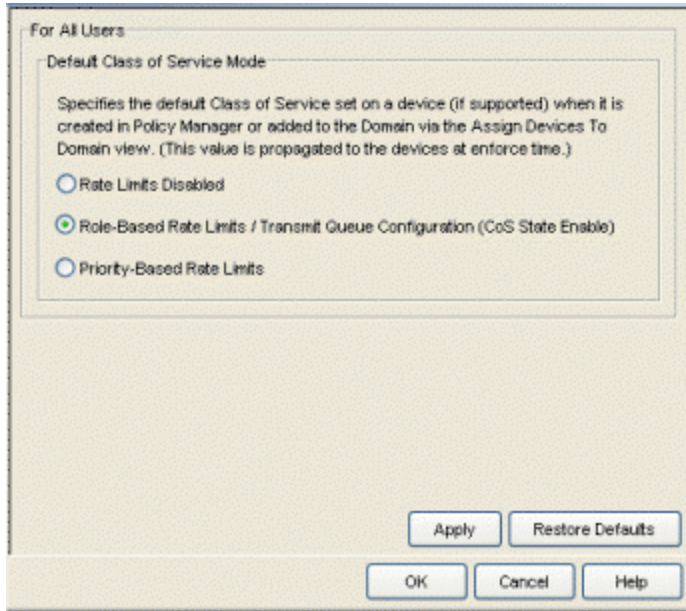
Selecting Default Class of Service in the left panel of the Options window (Tools > Options) provides the following view where you can specify the default Class of Service mode to set on a device (if supported) when it is created in Policy Manager or added to the domain via the Assign Devices to Domain window. The default setting is "Role-Based Rate Limits/ Transmit Queue Configuration." The CoS mode is written to the devices when an Enforce operation is performed. This setting applies to all users.

See below for information about the three selections.

---

**NOTE:** You can change this default value for a specific device by setting a different CoS mode in the [Device General tab](#) or via the Device Configuration Wizard.

---



Select the class of service mode or select the option to disable rate limits on devices. Only certain devices such as the N-Series Gold and Platinum devices support both modes, but you cannot have both modes enabled at the same time. See [Getting Started with Class of Service](#) for more information.

### Rate Limits Disabled

Select this option if you want rate limits disabled. This means that any priority-based rate limits will not be written to devices on enforce, and any role-based rate limits will not be included in roles written to devices on enforce.

### Role-Based Rate Limits/Transmit Queue Configuration

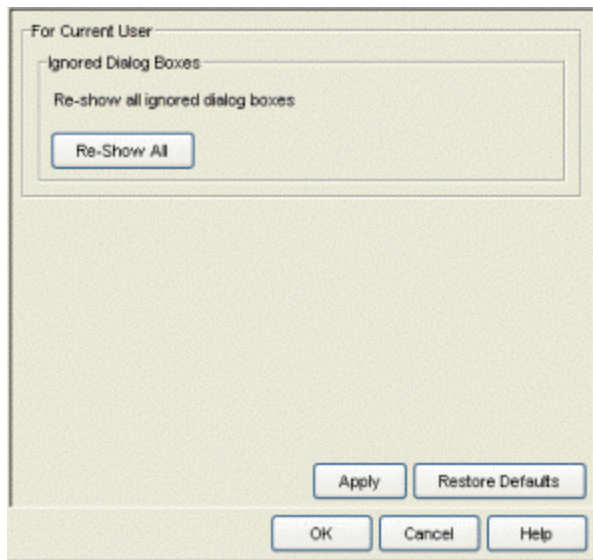
Select this mode if you want to be able to configure role-based rate limits and transmit queues on devices. These rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the class of service. See [How to Define Rate Limits](#) and [How to Configure Transmit Queues](#) for more information.

### Priority-Based Rate Limits

Priority-based rate limits are supported in Policy Manager for use with legacy devices such as the E7 and E1 devices. See [Priority-Based Rate Limits](#) for more information.

## Dialog Boxes

Selecting Dialog Boxes in the left panel of the Options window (Tools > Options) provides the following view where you can turn on the message dialog boxes that you have turned off on individual dialog box(es). This setting applies only to the current user.

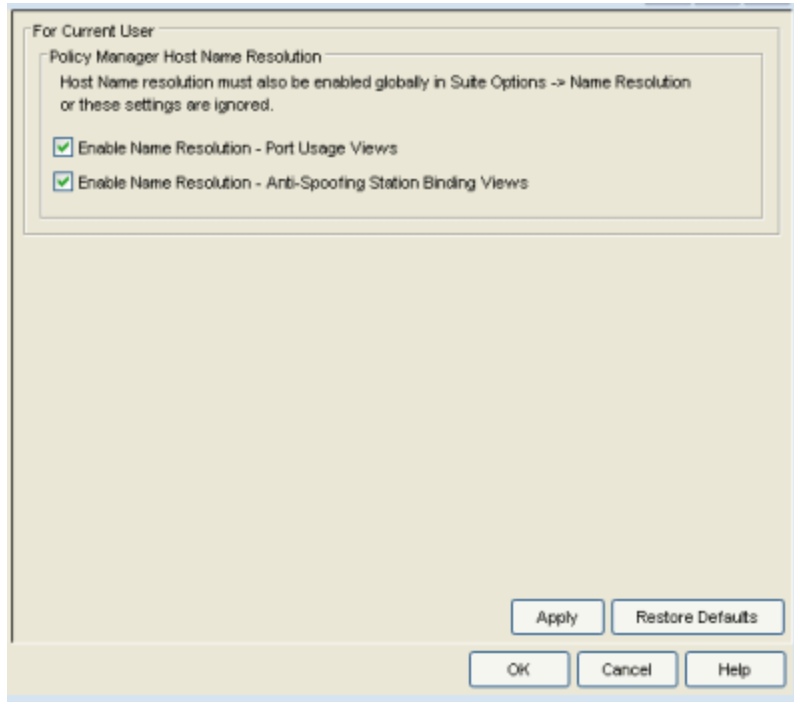


## Name Resolution (PM)

Selecting Name Resolution (PM) in the left panel of the Options window (Tools > Options) provides the following view where you can enable or disable host name resolution for Policy Manager Port Usage tabs and Anti-Spoofing binding views.

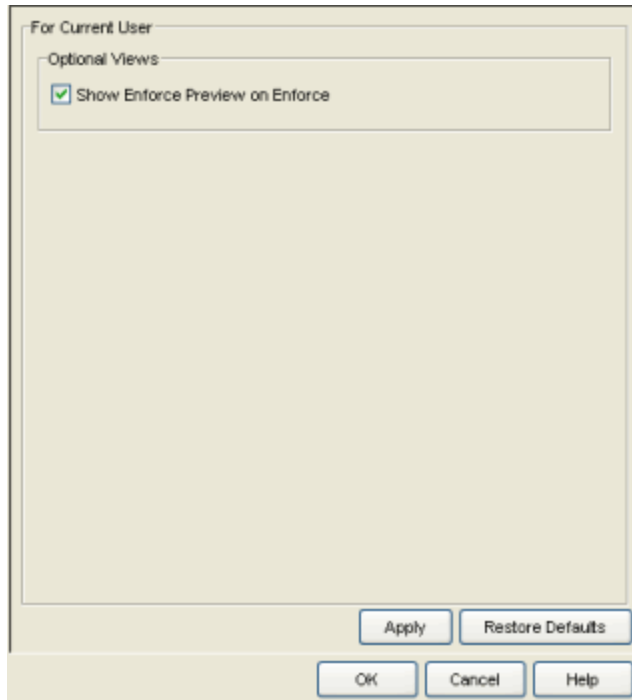
Host name resolution must also be enabled globally in the Suite Options > Name Resolution panel or these settings are ignored.

These options are enabled by default, but can be turned off for diagnostic or troubleshooting purposes, if needed.



## Optional Views

Selecting Optional Views in the left panel of the Options window (Tools > Options) provides the following view where you can choose whether or not you want certain views to be displayed. These settings apply only to the current user.



### Enforce Preview

When this checkbox is checked, the [Enforce Preview window](#) will appear any time you [enforce](#), before the actual enforcement takes place. You can also turn this option on and off on the Enforce Preview window itself.

## Policy Rule Hit Reporting

Selecting Policy Rule Hit Reporting in the left panel of the Options window (Tools > Options) provides the following view where you can configure the Policy Rule Hit Reporting feature. This feature allows you to view reports on rule usage for your policy domains. The reports can be accessed from the View menu. To use rule hit reporting, the devices must be configured to do rule accounting via the device [Role/Rule tab](#), and each rule in the domain must have the Generate System Log on Rule Hit option selected on the rule [General tab](#). For more information on configuring Policy Rule Hit Reporting, see [Rule Accounting and Rule Hit Reporting](#).

The screenshot shows a window titled "Policy Manager Options Window" with two main sections: "For All Users" and "For Current User".

**For All Users**

NetSight Policy Rule Hit Reporting allows the end user to view reports on rule usage for Policy Domains. The rule hit data is collected through syslog messages and stored in the NetSight database.

Once Policy Rule Hit Reporting is enabled, the devices must be configured to do rule accounting and send syslog messages to the NetSight server. (See the device Role/Rule tab for setup.)

Server Policy Rule Hit Reporting

Database Aging Row Count: 1000000

Syslog Message Queue Drain Size: 3000

**For Current User**

Client Reporting View Options

Real Time View Maximum Table Size: 10000

Policy Accounting View Polling Interval: 1800

Policy Accounting View Maximum Table Size: 5000

Buttons: Apply, Restore Defaults, OK, Cancel, Help

### Database Aging Row Count

Once every 24 hours (based on when the server is started), the policy rule hit database table is trimmed to no more than the row count (number of entries) specified here. This prevents the table from getting too large. This setting is for all users.

### Syslog Message Queue Drain Size

Specifies the maximum number of rule hits written to the database by the reporting agent every two seconds. The reporting agent has a message queue that stores all the rule hits from the syslog server. Every two seconds the queue is drained and the messages are written to the database. The Syslog message drain queue size limits the number of rule hits that can be written to the database. This prevents the reporting agent from monopolizing the database in the case of a deny attack on the network, where many rule hits could be generated at one time. This setting is for all users.



### Real Time View Maximum Table Size

The maximum number of rows allowed in the Real Time Policy Rule Hits table (View > Policy Rule Hit > Real Time Policy Rule Hits). The oldest rows are aged out when new ones come in. This setting is for the current user only.

### Policy Accounting View Polling Interval

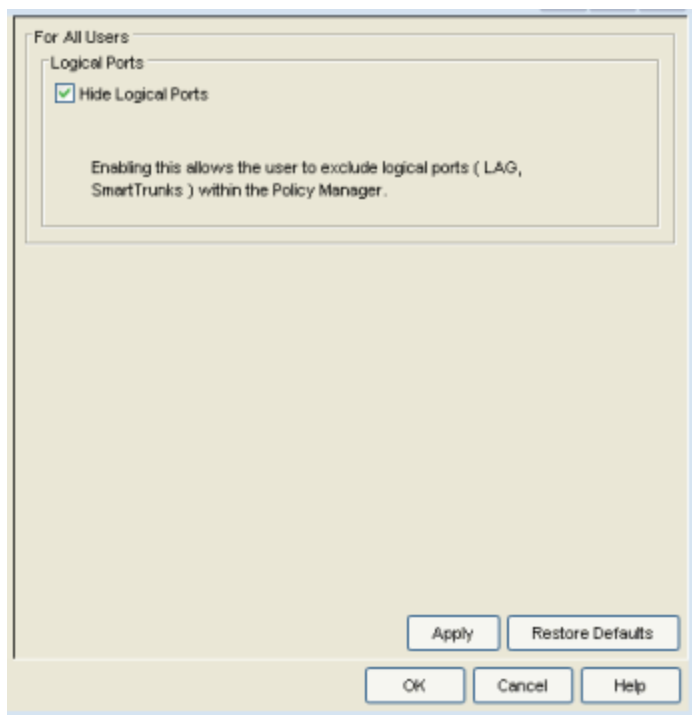
Use this option to set the polling interval for the Policy Rule Hit Accounting tool. This tool shows all rule hits read from latest data in the database and can be accessed by selecting the View menu > Policy Rule Hit > Policy Accounting Tool. The polling interval is the frequency of the database query. This setting is for the current user only.

### Policy Accounting View Maximum Table Size

The maximum number of rows allowed in the tables displayed in Policy Rule Hit Reports (View > Policy Rule Hit). The oldest rows are aged out when new ones come in. This setting is for the current user only.

## Ports

Selecting Ports in the left panel of the Options window (Tools > Options) provides the following view where you can set or clear the Hide Logical Ports feature. This setting applies only to the current user.



## Hide Logical Ports

The Hide Logical Ports feature lets you hide the display of logical ports in Policy Manager. Logical ports include SmartTrunk ports and LEC (LAN emulation client) ports, which can be seen in Policy Manager even if they are not yet configured or connected. If there are too many of these logical ports, they can cause unwanted clutter in your Policy Manager port list displays.

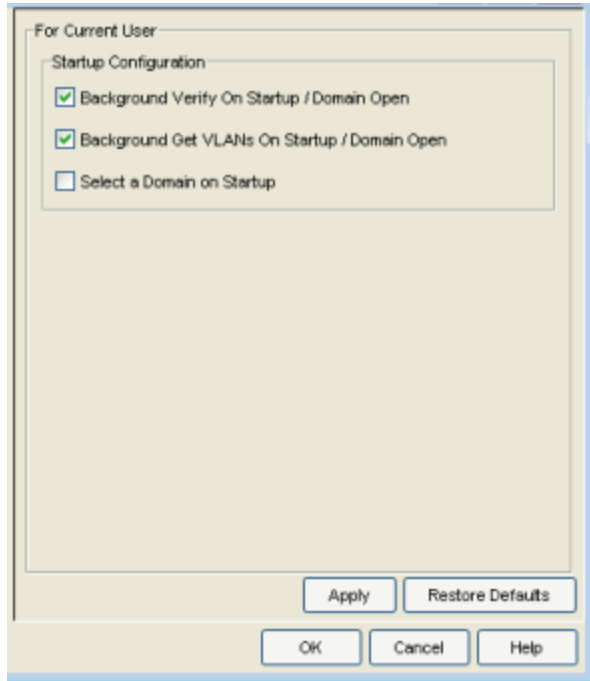
## Startup

Selecting Startup in the left panel of the Options window (Tools > Options) provides the following view where you can configure the features that run on startup.

When you launch Policy Manager or open a domain, two background operations are automatically performed: a background read of the VLANs from all reachable devices and a background verify operation that determines if the roles on the devices match those in the current Policy Manager domain. Because these operations run in the background, you have instant access to Policy Manager and the domain even while the operations are verifying the current status of the domain. However, you can deselect the options in this view to prevent these operations from being performed, if desired. (For more information on the verify operation, see [Verifying](#) in the Policy Manager Concepts file.)

In addition, you can set an option that allows you to select a domain on startup. When you start Policy Manager, the Select a Domain to Open window presents a drop-down list that allows you to select which domain to open, or create a new domain, if desired. If this option is not selected, Policy Manager will open the domain that was open when the NetSight client last closed.

These settings apply only to the current user.



### Background Verify On Startup/Domain Open

Deselect this option to stop a background verify operation that is performed when Policy Manager is launched or when you open a domain.

### Background Get VLANs On Startup/Domain Open

Deselect this option to stop a background operation to read the VLANs from all reachable devices that is performed when Policy Manager is launched or when you open a domain.

### Select a Domain On Startup

Select this option if you want to select a domain to open when Policy Manager is launched.

## SNMP Options

Selecting SNMP Options in the left panel of the Options window (Tools > Options) provides the following view where you can specify SNMP polling parameters for the Policy Manager server and client.

For All Users

Server SNMP

SNMP Retries: 3

SNMP Timeout: 3 seconds

Enforce/Verify

Force read of policy rules table

For Current User

Client SNMP

SNMP Retries: 3

SNMP Timeout: 3 seconds

Apply Restore Defaults

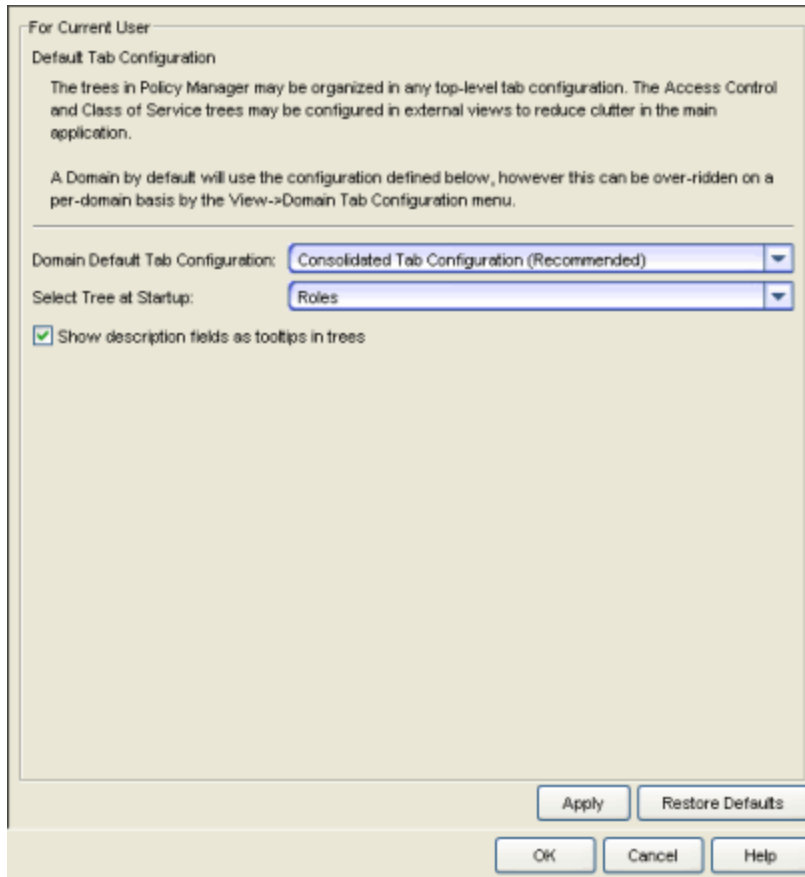
OK Cancel Help

### Enforce/Verify

To improve performance time during the verify operation, Policy Manager uses the "Last Changed" attribute on the device to determine if any rules have changed. Selecting the "Force read of policy rules table" option causes Policy Manager to perform the verify operation using the rules table instead of the attribute. This can cause the verify operation to take longer to perform. Normally this option is not selected and should only be enabled for specific customer deployments as instructed by Extreme Networks Support.

## Tab Configuration

Selecting Tab Configuration in the left panel of the Options window (Tools > Options) provides the following view where you can specify the top-level tab organization for your domains. By default, all domains will use the configuration defined here. However, it is possible to override these setting on a per-domain basis using the View > [Domain Tab Configuration](#) menu. Any new domain you create will use the settings specified here. These settings apply only to the current user.



## Domain Default Tab Configuration

Use the drop-down list to select the tab configuration you would like to use in your domains:

- Consolidated Tab Configuration (Recommended) - In this configuration, there are two top-level tabs: Roles/Services and Network Elements/Port Groups. Access Control and Class of Service trees are presented in external Configuration windows accessed from the Edit menu.
- Classic Tab Configuration - This configuration uses six top-level tabs, one for each Policy Manager tree: Roles, Services, Access Control, Classes of Service, Network Elements, and Port Groups. This is similar to the configuration used in Policy Manager prior to version 4.0.
- Custom Tab Configuration - This configuration allows you to define which tab the different Policy Manager trees will be organized under. For Access Control and Classes of Service trees, you can also select to

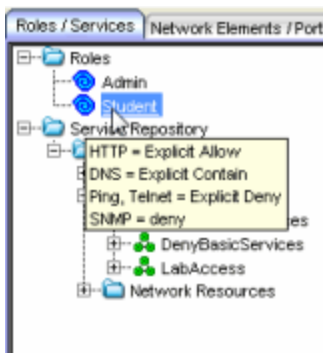
display the tree in a Configuration View (an external window) accessed from the Edit menu.

### Select Tree at Startup

Specify the tree that will be selected in the left-panel when you start Policy Manager.

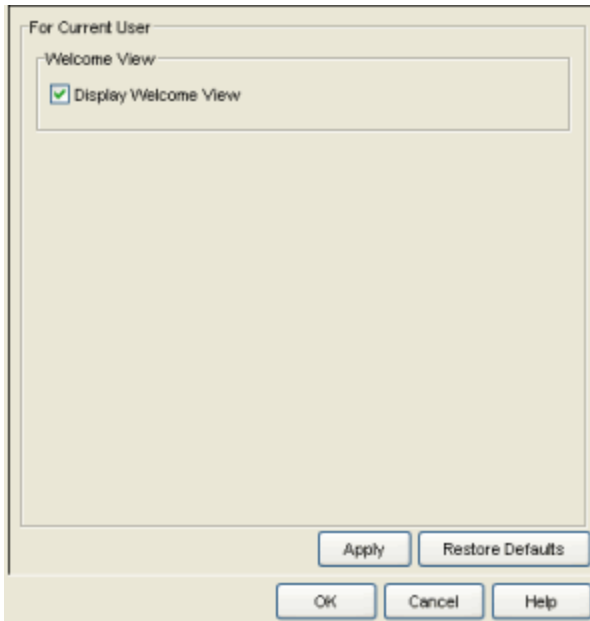
### Show description fields as tooltip in trees

If this option is selected, a description of each node in a tree will be displayed (if available) in a tooltip when the cursor hovers over the node. In the example below, you can see that a description of the Student role is displayed when the cursor hovers over the Student node in the tree.



## Welcome View

Selecting Welcome View in the left panel of the Options window (Tools > Options) provides the following view where you can display or hide the Welcome tab that is displayed when you first open Policy Manager. This setting applies only to the current user.



## Wireshark

Selecting Wireshark in the left panel of the Options window (Tools > Options) provides the following view where you can specify the location of the Wireshark executable so that it can be used by Policy Manager to display rule color filters. For more information on using Wireshark in Policy Manager, see [How to Use Wireshark to Analyze a Role's Behavior](#). This setting applies only to the current user.



## **Related Information**

For information on related tasks:

- [How to Set Policy Manager Options](#)



## Port Properties Anti-Spoofing Tab

---

The Port Properties Anti-Spoofing tab lets you enable or disable the anti-spoofing feature on the selected port, if the device supports it.

There are two ways to access the Anti-Spoofing tab:

- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the Anti-Spoofing tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the Anti-Spoofing tab in the right panel.

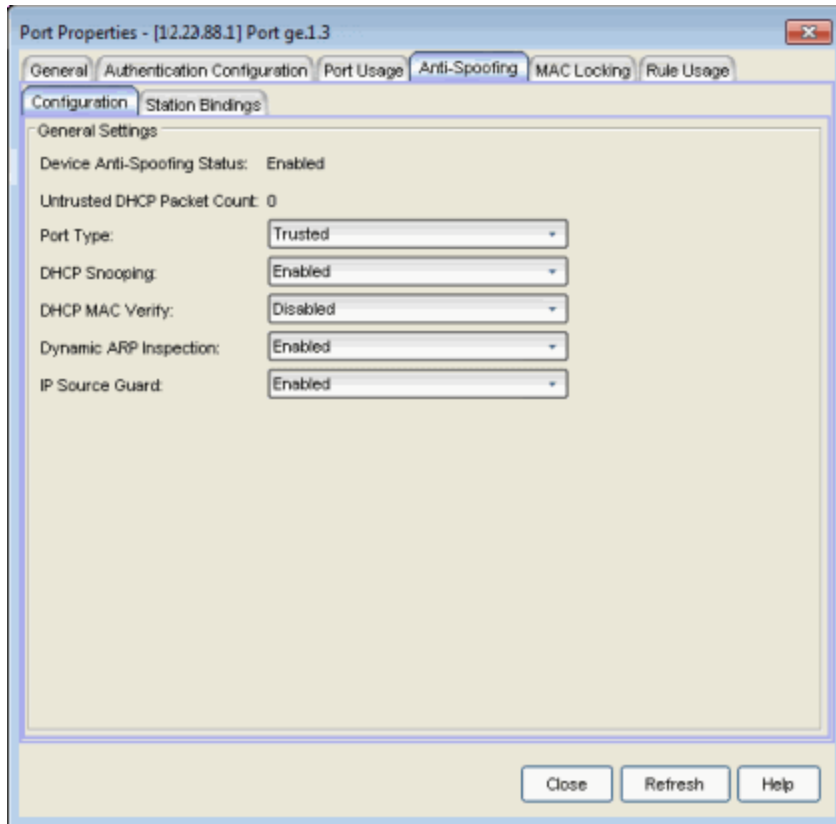
In order for Anti-Spoofing to take effect on a port, it must be enabled at the device level. You can do this using the device [Anti-Spoofing tab](#).

The Port Properties Anti-Spoofing tab provides two sub-tabs:

- [Configuration Tab](#)
- [Station Bindings Tab](#)

### Configuration Tab

This tab lets you enable/disable the different anti-spoofing methods on the port as well as view the anti-spoofing status on the device. If the device does not support anti-spoofing, these options are grayed out.



### Device Anti-Spoofing Status

Shows whether the anti-spoofing feature is enabled or disabled the device. In order for anti-spoofing to take effect on a port, it must be enabled at the device level. You can do this using the device [Anti-Spoofing tab](#).

### Untrusted DHCP Packet Count

The number of DHCP server packets received on this port. This counter will only increment when the Port Type is set to untrusted.

### Port Type

The DHCP snooping port type determine anti-spoofing behavior:

**Trusted** - DHCP server traffic is accepted and used to create bindings in the MAC-to-IP address binding table. Typically, only a port that is connected to a DHCP server would be set to trusted.

**Bypass** - Snooping of DHCP server traffic does not take place on the port. Typically, uplink ports out to the network would be set to bypass, as traffic would not be originating from that port.

**Untrusted** - The untrusted server counter is incremented when DHCP server traffic (DHCP ACK) is detected on the port, and the packets are

dropped. DHCP RELEASE and DECLINE messages, sent by a client to free its IP address for use by another, are dropped if they are for a MAC address in the binding table that is on another port. If [DHCP MAC Verify](#) is enabled and the source MAC address does not match the Client Host Address in the DHCP payload (CHADDR), the packets are dropped. Typically, all edge ports with users would be set to untrusted.

#### DHCP Snooping

Whether [DHCP Snooping](#) is enabled or disabled on the port.

#### DHCP MAC Verify

Whether [DHCP MAC Verify](#) is enabled or disabled on the port.

#### Dynamic ARP Inspection

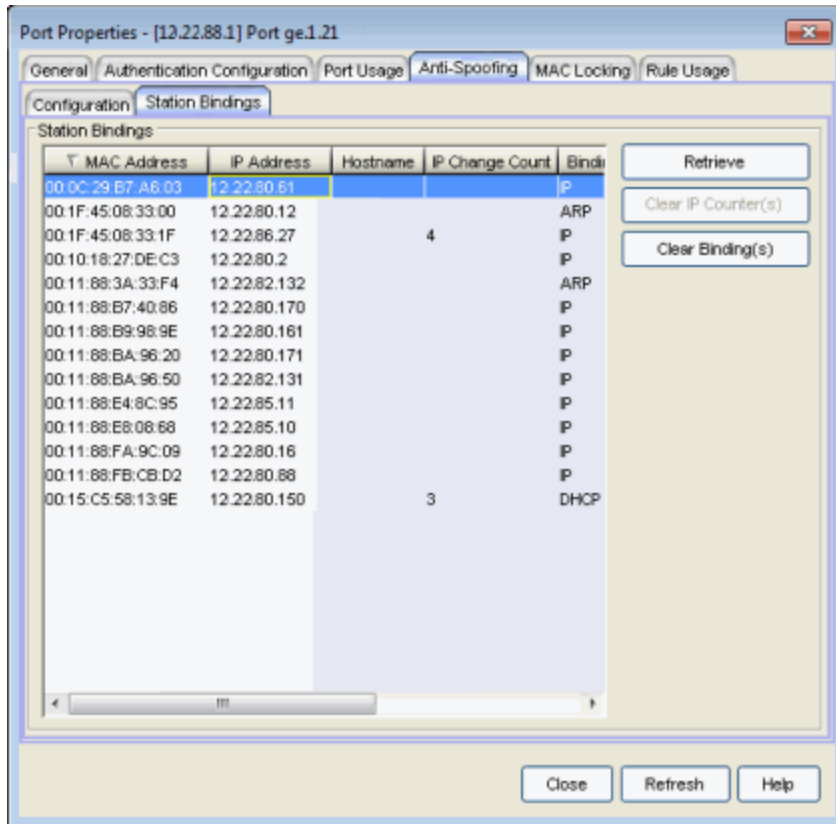
Whether [Dynamic ARP Inspection](#) is enabled or disabled on the port. When set to inspection only, Dynamic ARP inspection will occur, but will not be used to create bindings.

#### IP Source Guard

Whether [IP Source Guard](#) is enabled or disabled on the port. When set to inspection only, IP Source Guard will occur, but will not be used to create bindings.

## Station Bindings Tab

This tab presents a table that displays the current active bindings for the port set up through anti-spoofing. These bindings are the valid MAC/IP/Port associations detected on trusted ports from the various anti-spoofing methods such as DHCP snooping. This tab also provides the ability to reset violation counters and clear bindings from the table. You must click the **Retrieve** button to display the bindings information.



### MAC Address

The MAC address of the binding.

### IP Address

The IP address of the binding.

### Hostname

An administratively-assigned hostname for the device.

### IP Change Count

The number of times the IP address has changed for this binding.

### Binding Type

Indicates which binding type (DHCP, ARP, or IP inspection) was used to create the entry.

### Duration (sec)

The amount of time, in seconds, that this binding has been operational for.

### Lease Time (sec)

The amount of time, in seconds, that this binding will be operational before being destroyed. A value of zero (0) indicates that this binding will not

expire.

**Retrieve**

Retrieves the bindings for the device.

**Clear IP Counter(s)**

Resets the IP Change Count to zero for the binding.

**Clear Binding(s)**

Removes the binding from the table.

---

**Related Information**

For information on related tasks:

- [How to Configure Anti-Spoofing](#)
- [Device Anti-Spoofing Tab](#)

## Port Properties Authentication Configuration Tab

---

The Port Properties Authentication Configuration tab allows you to configure and change the [authentication](#) settings for a port. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect. Only those areas of the tab that relate to the authentication type configured on the device are available for editing.

There are two ways to access the Authentication Configuration tab:

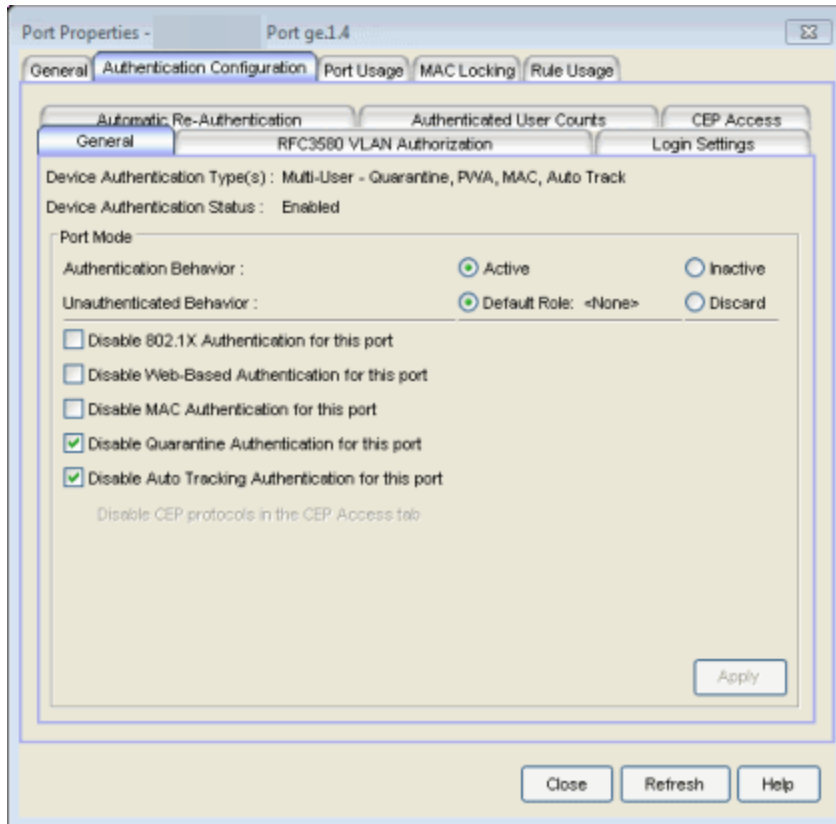
- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the Authentication Configuration tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the Authentication Configuration tab in the right panel.

The Authentication Configuration tab has six sub-tabs:

- [General Tab](#)
- [RFC3580 VLAN Authorization Tab](#)
- [Login Settings Tab](#)
- [Automatic Re-Authentication Tab](#)
- [Authenticated User Counts Tab](#)
- [CEP Access Tab](#)

### General Tab

This tab displays general authentication and port mode information about the port.



### Device Authentication Type(s)

Authentication type(s) configured on the device ([Quarantine](#), [802.1X](#), [Web-Based](#), [MAC](#), [Auto Track](#), or None). Some devices support multiple authentication types and multiple users (Multi-User authentication) per port, while others are restricted to only one or two authentication types and single users per port (Single User authentication). If the value is None, all types of authentication are disabled at the device level, and port authentication settings cannot be configured and will not take effect.

### Device Authentication Status

Indicates whether or not the authentication type(s) configured on the device are enabled or not. If multiple authentication types are configured on the device, this status applies to all authentication types. If authentication is disabled at the device level, port authentication settings will not take effect.

### Port Mode

This area displays the current port mode for the port, and allows you to change the settings if desired. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a

combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to the port's default role or discarded). See [Port Mode](#) for a complete description of each port mode.

In addition, this section provides checkboxes that allow you to disable a specific authentication type at the port level.

### Authentication Behavior

Select an option to specify whether or not authentication is enabled on the port. (See [Port Mode](#) for more information.) If you set the port's Authentication Behavior to Active (i.e., you enable authentication for the port), it is recommended that you enable the [Drop VLAN Tagged Frames](#) feature.

**NOTE:** Authentication Behavior must be set to Active for authentication to be allowed using CEP Protocols.

### Unauthenticated Behavior

Select an option to specify whether unauthenticated traffic will be assigned to the port's [default role](#) or discarded. The current default role for the port is shown. For additional information, see [Port Mode](#).

---

**NOTE:** For Single User 802.1X and 802.1X+MAC authentication types:

- Active/Default Role mode requires that a default role be set on the port.
- Active/Discard mode requires that any default role set on the port is cleared.

For Multi-User Web-based authentication:

- Active/Discard mode is not supported.
- 

### Disable 802.1X Authentication for this port

Select this checkbox to disable 802.1X authentication at the port level. If the device is only configured with 802.1X authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

**NOTE:** For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port will not be able to authenticate via 802.1X or MAC. The port will behave as if Inactive/Default Role is the selected port mode.

### Disable Web-Based Authentication for this port

Select this checkbox to disable web-based authentication at the port level. If the device is only configured with web-based authentication, selecting



this checkbox will result in the port Authentication Behavior being set to Inactive.

---

**NOTE:** For Multi-User Web-Based authentication with Active/Discard as the selected port mode: This checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

---

#### Disable MAC Authentication for this port

Select this checkbox to disable MAC authentication at the port level. If the device is only configured with MAC authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

#### Disable CEP protocols in the CEP Access tab

Use the [CEP Access tab](#) to disable CEP protocols at the port level.

#### Disable Quarantine Authentication for this port

Select this checkbox to disable Quarantine authentication at the port level. If the device is only configured with Quarantine authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

#### Disable Auto Tracking Authentication for this port

Select this checkbox to disable MAC authentication at the port level. If the device is only configured with Auto Tracking authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

#### Apply Button

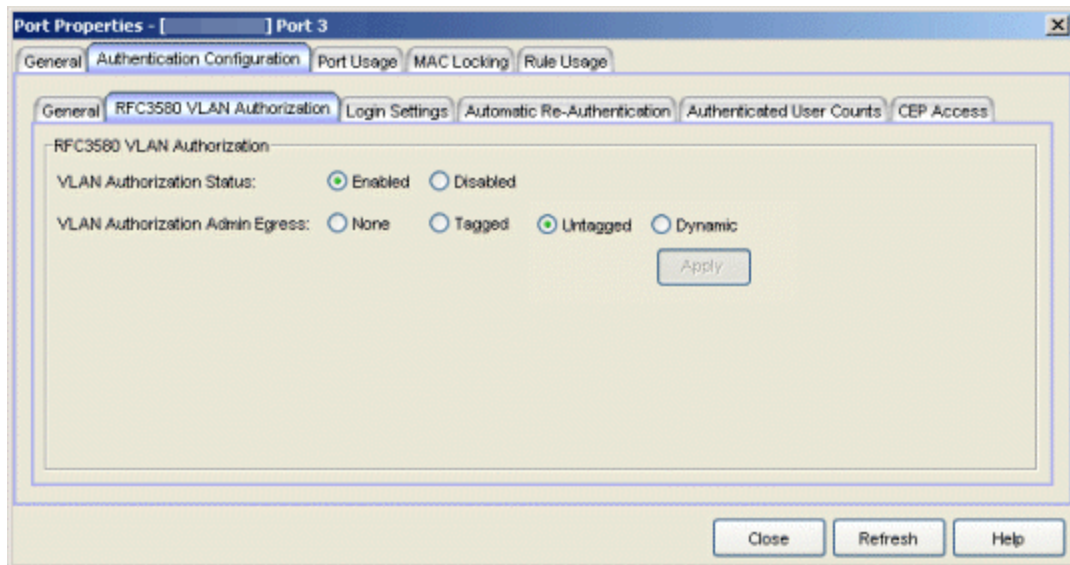
Applies any Port Mode changes to the port.

## RFC3580 VLAN Authorization Tab

This tab lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy, will tag packets with the VLAN ID.
- ports on devices that do support policy and also support [Authentication-Based VLAN to Role Mapping](#), will classify packets according to the role that the VLAN ID maps to.

You can also enable and disable VLAN Authorization at the device level using the device [Authentication tab](#). If the device does not support RFC 3580, this tab will be grayed out.



### VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

### VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

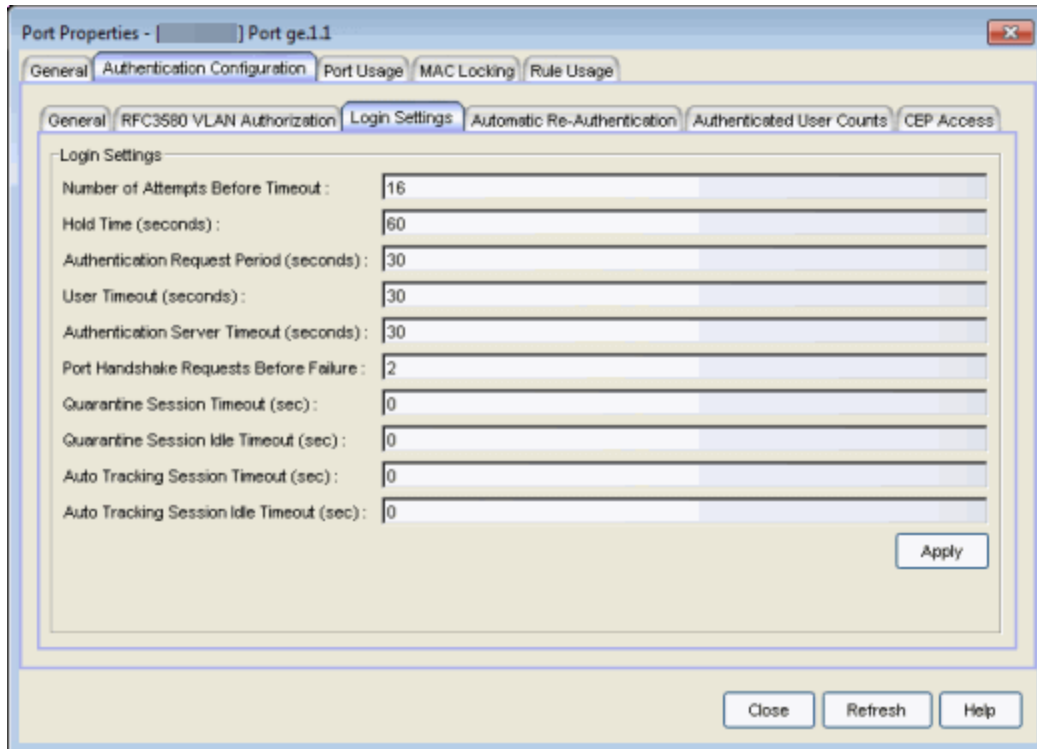
The current egress settings for the port are displayed in the [VLAN Oper Egress column](#) in the End User Sessions table on the Port Usage tabs. These options are grayed out if not supported by the device.

### Apply Button

Saves any change you made to the VLAN Authorization settings.

## Login Settings Tab

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



The screenshot shows a window titled "Port Properties - [ ] Port ge.11". The "Authentication Configuration" tab is selected, and within it, the "Login Settings" sub-tab is active. The "Login Settings" section contains the following fields:

Field	Value
Number of Attempts Before Timeout :	16
Hold Time (seconds) :	60
Authentication Request Period (seconds) :	30
User Timeout (seconds) :	30
Authentication Server Timeout (seconds) :	30
Port Handshake Requests Before Failure :	2
Quarantine Session Timeout (sec) :	0
Quarantine Session Idle Timeout (sec) :	0
Auto Tracking Session Timeout (sec) :	0
Auto Tracking Session Idle Timeout (sec) :	0

Buttons for "Apply", "Close", "Refresh", and "Help" are visible at the bottom of the window.

### Number of Attempts Before Timeout

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2. For 802.1X and MAC authentication, this value is permanently set to 1.

### Hold Time (seconds)

Amount of time (in seconds) authentication will remain timed out after the specified Number of Attempts Before Timeout has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

### Authentication Request Period

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then

attempts to authenticate the user. Valid values are 1-65535. The default is 30.

#### **User Timeout**

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

#### **Authentication Server Timeout**

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

#### **Port Handshake Requests Before Failure**

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user, before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

#### **Quarantine Session Timeout (sec)**

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

#### **Quarantine Session Idle Timeout (sec)**

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

#### **Auto Tracking Session Timeout (sec)**

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

#### **Auto Tracking Session Idle Timeout (sec)**

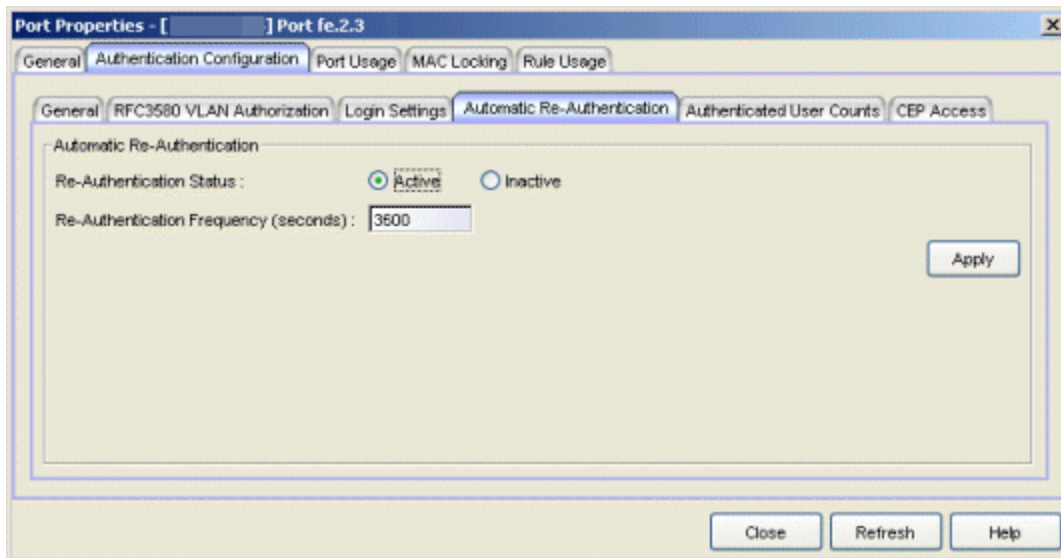
For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

#### **Apply Button**

Applies the Login Settings changes to the port.

## Automatic Re-Authentication Tab

This tab is grayed-out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information, to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."



### Re-Authentication Status

If Active is selected, the re-authentication feature is enabled. If Inactive is selected, the re-authentication feature is disabled.

### Re-Authentication Frequency

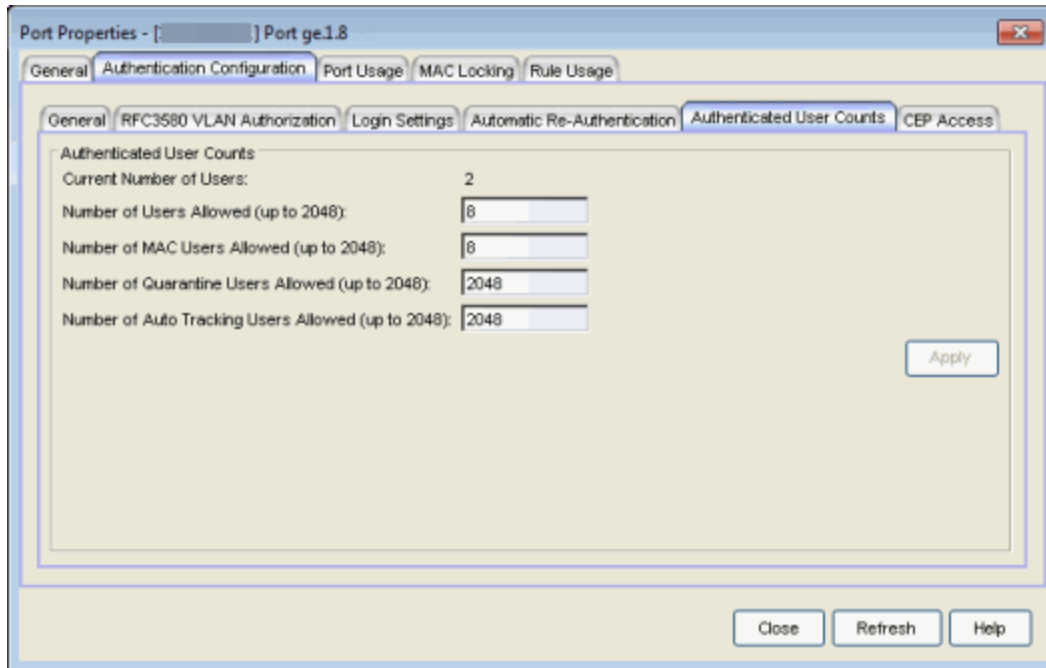
How often (in seconds) the device checks the port to re-authenticate the logged in user. Valid values are 1-2147483647. The default is 3600.

### Apply Button

Applies the Automatic Re-Authentication changes to the port.

## Authenticated User Counts Tab

This tab provides authenticated user count information for devices with Multi-User as their configured authentication type. See the [device Authentication tab](#) for information on setting the device authentication type.



### Current Number of Users

The current number of users that are actively authenticated or have authentications in progress on this interface. If multi-user authentication is disabled, this number will be 0 (zero). Any unauthenticated traffic on the port is not included in this count.

### Number of Users Allowed (up to 2048)

The number of users that can be actively authenticated or have authentications in progress at one time on this interface. If you set this value below the current number of users, end user sessions exceeding that number will be terminated.

---

**NOTE: B2/C2 Devices.** If you are configuring a single user and an IP phone per port, set this value to 2.

---

### Number of MAC Users Allowed (up to 2048)

The number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If MAC is not selected as a Multi-User authentication type on the [device Authentication tab](#), this field will be grayed out.

### Number of Quarantine Users Allowed (up to 2048)

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Quarantine Auth is not enabled on the [device Authentication tab](#), this field will be grayed out.

### Number of Auto Tracking Users Allowed (up to 2048)

The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Auto Tracking is not enabled on the [device Authentication tab](#), this field will be grayed out.

### Apply Button

Applies User Counts changes to the port.

## CEP Access Tab

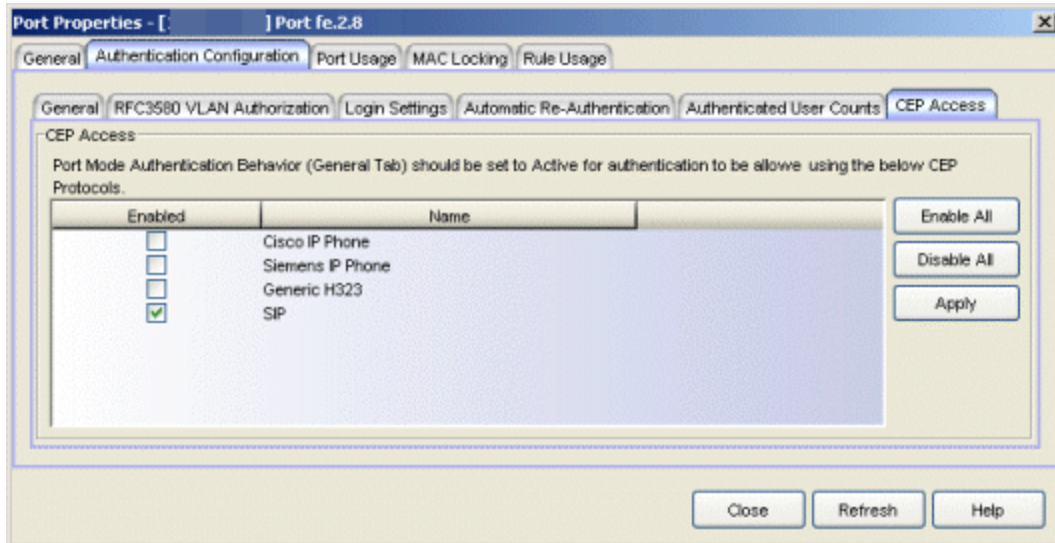
This tab lists all the CEP (Convergence End Point) protocols supported by the device that the port resides on, and lets you enable or disable them for that port. For devices that do not support CEP, the tab will be blank.

---

**NOTE:** Port Mode Authentication Behavior must be set to Active (on the [General sub-tab](#)) for authentication to be allowed using these CEP Protocols.

---

You can enable CEP protocols for multiple ports using the [Port Configuration Wizard](#). In addition to enabling protocols on the port, you must also configure CEP for the device the port resides on. You can configure CEP for a single device using the [device Authentication tab \(CEP sub-tab\)](#) or for multiple devices using the [Device Configuration Wizard](#).



### CEP Access

Lists all the CEP protocols supported by the device that the port resides on. Use the checkboxes to enable or disable CEP protocols on this port. If the device does not support the CEP feature, this area is blank.

### Enable All Button

Selects all the checkboxes and enables all the CEP protocols for this port.

### Disable All Button

Deselects all the checkboxes and disables all the CEP protocols for this port.

### Apply Button

Applies CEP access changes to the port.

---

## Related Information

For information on related tasks:

- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)

For information on related tabs:

- [Port Properties - Port Usage Tab](#)
- [Port Properties - General Tab](#)



## Port Properties General Tab

---

The Port Properties General tab provides general information about the selected port, and also lets you view and change various port configuration settings.

There are two ways to access the General tab:

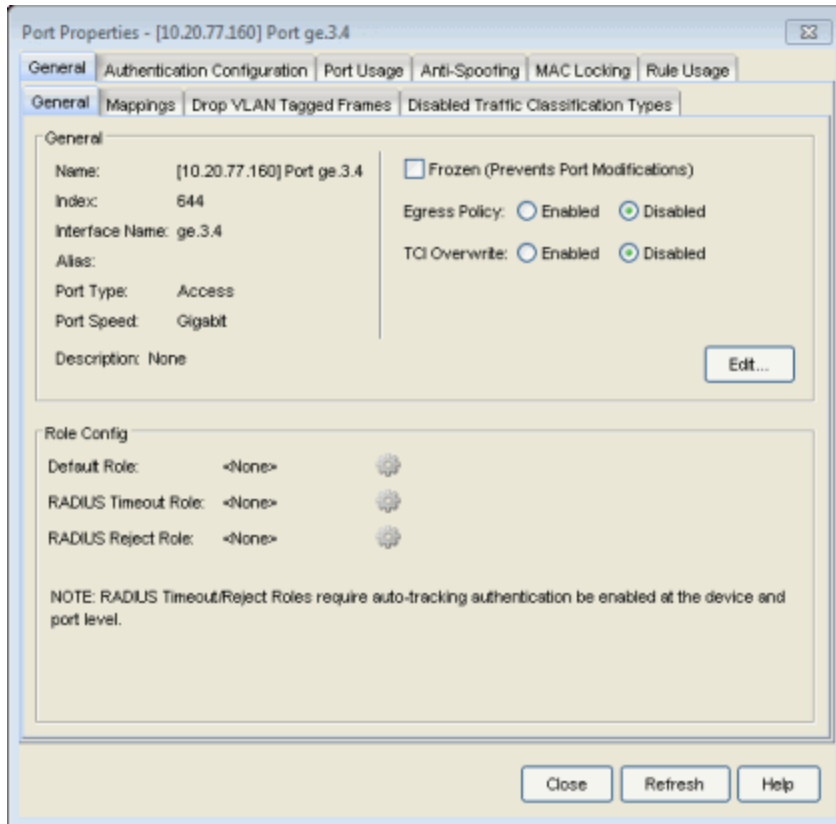
- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the General tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the General tab in the right panel.

The General tab has four sub-tabs:

- [General Tab](#)
- [Mappings Tab](#)
- [Drop VLAN Tagged Frames Tab](#)
- [Disabled Traffic Classification Types Tab](#)

### General Tab

This tab displays general information about the port and indicates whether it is a frozen port or if TCI Overwrite is enabled on the port.



## General

### Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

### Index

The index value assigned to the port interface.

### Interface Name

A description of the port.

### Alias

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

### Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

### Port Speed

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

### Frozen (Prevents Port Modifications)

Enables you to freeze (check) the port or clear (uncheck) the frozen status on the port. Freezing a port "locks" it so that no one can accidentally reconfigure sensitive attributes such as port authentication or default role settings, or terminate sessions that are authenticated on the port. See [How to Freeze/Unfreeze a Port](#) for more information.

### Egress Policy

Enable or disable Egress Policy for the port. (This option will be grayed out if the device on which the port is located does not support egress policy.) Egress policy can be used in scenarios where policy may not be in force at the user edge throughout the entire network. For example, a policy can be created that prevents users from running unauthorized Apache web servers. If an end user has an Apache server running on their end-system (where policy is in use), an egress policy could prevent another end-system (where policy is not in use) from accessing that end-system as an HTTP server, by dropping HTTP queries destined to that end user. Egress policy works in conjunction with the ingress policy configured for the port, in that the same ingress policy rules will be applied to the traffic egressing the port, with the exception of rules that specify a source or destination address. In this case, the ingress rules will still be used, but the direction of the rule will be inverted on egress. For example, an ingress MAC Address Source rule will match the destination MAC address of the frame on egress. If you enable egress policy, you must also enable TCI Overwrite.

### TCI Overwrite

Enable or disable TCI Overwrite functionality for the port. (This option will be grayed out if the device on which the port is located does not support TCI Overwrite.) Enabling TCI Overwrite causes the VLAN or class of service tag in a received packet to be overwritten by the VLAN (access control) and class of service characteristics defined in the port's current or default role. If there is no role assigned to the port, the port uses any static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. TCI Overwrite is required for some devices for Tagged Packet [VLAN to Role Mapping](#), and can be enabled either here on a per-port basis, or for an individual role in the role's [General tab](#), as well as on a per-rule basis in the [Rule General Tab](#).

### Description

Use the **Edit** button to add or change a description of the port. For example, you could use the description field to explain why a port is frozen. This description can then be viewed as a tooltip when you hover over the

port nodes in the tree (when under a port group) as well as in the right-panel Ports and Details View tabs.

### *Role Config*

This section displays the default role on the port, and lets you select a new default role, as well as a RADIUS Timeout role and RADIUS Reject role for the port. These options allow you to specify a different policy role for each possible outcome of the authentication process.

Click on the gear icon  to open a window where you can select the role.

---

**NOTE:** The RADIUS Timeout Role and RADIUS Reject Role features require that auto-tracking authentication be enabled at the device and port level in order to be operational.

---

#### Default Role

Select a role to assign as the port's default role. The default role is the role assigned to the port if no other role has been authenticated on it. If the port was not assigned a role when the end user logged in (authenticated), or if authentication is disabled on a port, then the port's default role will take effect. If you set a default role for the port, it is recommended that you enable the [Drop VLAN Tagged Frames](#) feature. See [Default Role](#) in the Concepts topic for information on default roles. For additional information, see [Port Mode](#).

#### RADIUS Timeout Role

Select the role to assign to the port if it encounters a RADIUS timeout. This allows you to assign a different role to end-systems that have not been provisioned on the network or that try to authenticate during a RADIUS outage. It also allows a different role to be assigned when RADIUS timeouts occur during re-authentication of multi-authentication sessions. This would allow user sessions to remain authenticated and provisioned when all RADIUS servers become unreachable due to an unexpected network outage.


#### RADIUS Reject Role

Select the role to assign to the port if it encounters a RADIUS reject. This can be used in scenarios where the Default role for a port provides lenient access privileges. If the port receives a RADIUS reject, then a RADIUS Reject role with limited or no access privileges would be assigned to the port to restrict the end user.

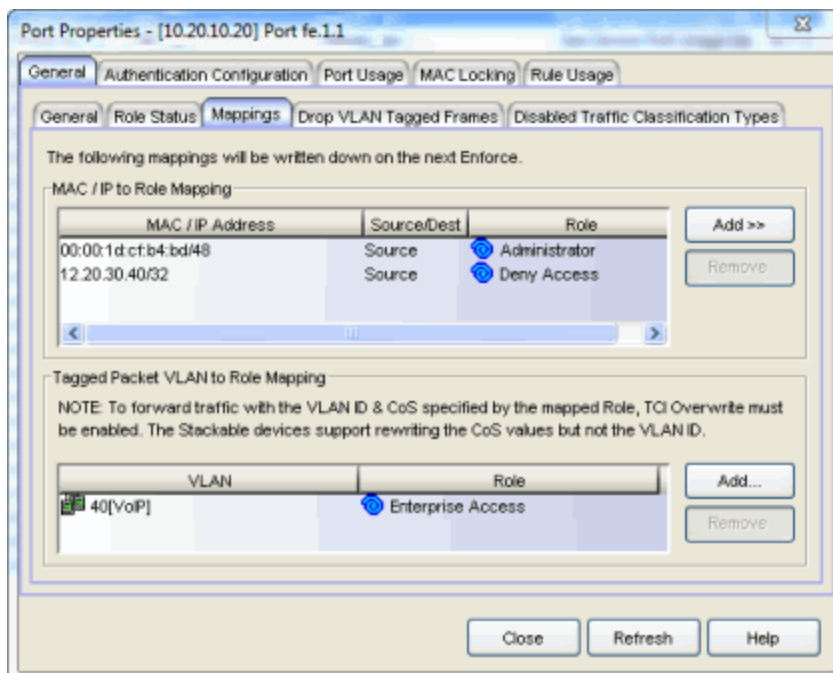
## Mappings Tab

This tab allows you to create port-level MAC or IP to Role mappings and Tagged Packet VLAN to Role mappings. A mapping does not have to exist at the device level to be created at the port level, and port-level mappings will override any device-level mappings. Any additions or changes you make to this tab must be [enforced](#) in order to take effect.

**NOTES:** You must have the Port Level Role Mappings feature enabled in Policy Manager for the mappings to take effect. (From the menu bar, select the Edit > Port Level Role Mappings checkbox.) If the feature is not enabled, the mappings will be ignored and any mappings listed here will be grayed out.

Port-level mappings cannot be added or removed to or from frozen ports . You must clear the frozen state on a port in order to add or remove a mapping. Once you have created a mapping, you can freeze the port. The port-level mappings of the frozen port will still be enforced and verified.

**WARNING:** Enforcing port-level MAC or IP to Role mappings could potentially remove rules created by NetSight Automated Security Manager (ASM) as an intrusion detection response.



### *MAC/IP to Role Mapping*

MAC or IP to Role mapping provides a way to assign a role to an end station based on its MAC or IP address. In this section, you can create a list of MAC or IP addresses and map each of them to a specific role. If the listed mappings are grayed out, it means that the Port Level Role Mappings feature is not enabled (Edit > Port Level Role Mappings).

#### **MAC/IP Address**

The MAC or IP addresses that are mapped to a role. Click **Add** to add a mapping to the list.

#### **Source/Destination**

Specifies whether the MAC/IP address is a source or destination address.

#### **Role**

The role that is mapped to a MAC/IP address. Click **Add** to add a mapping to the list.

#### **Add Button**

Use the Add button to add a MAC or IP to Role Mapping.

#### **Remove Button**

Select a MAC or IP address and click **Remove** to remove the address from the mapping list.

### *Tagged Packet VLAN to Role Mapping*

Tagged Packet VLAN to Role Mapping provides a way to assign a role to network traffic, based on a VLAN ID. In this section, you can create a list of VLANs and map each of them to a specific role. If the listed mappings are grayed out, it means that the Port Level Role Mappings feature is not enabled (Edit > Port Level Role Mappings). For more information, see [VLAN to Role Mapping](#) in the Concepts Help topic.

---

#### **NOTES: TCI Overwrite Requirement**

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingress with.

If supported by the device, you can enable TCI Overwrite on a per-port basis in the [Port Properties window General tab](#), or for an individual role in the role's [General tab](#). The stackable devices support rewriting the CoS values but not the VLAN ID.

---

**VLAN**

The VLANs (VLAN ID and name) that are mapped to a role. Click **Add** to add a mapping to the list.

**Role**

The role that is mapped to a VLAN. Click **Add** to add a mapping to the list.

**Add Button**

Opens the VLAN to Role Mapping Selection View, where you can select a VLAN and map it to a role.

**Remove Button**

Select a VLAN and click **Remove** to remove the VLAN from the mapping list.

## Drop VLAN Tagged Frames Tab

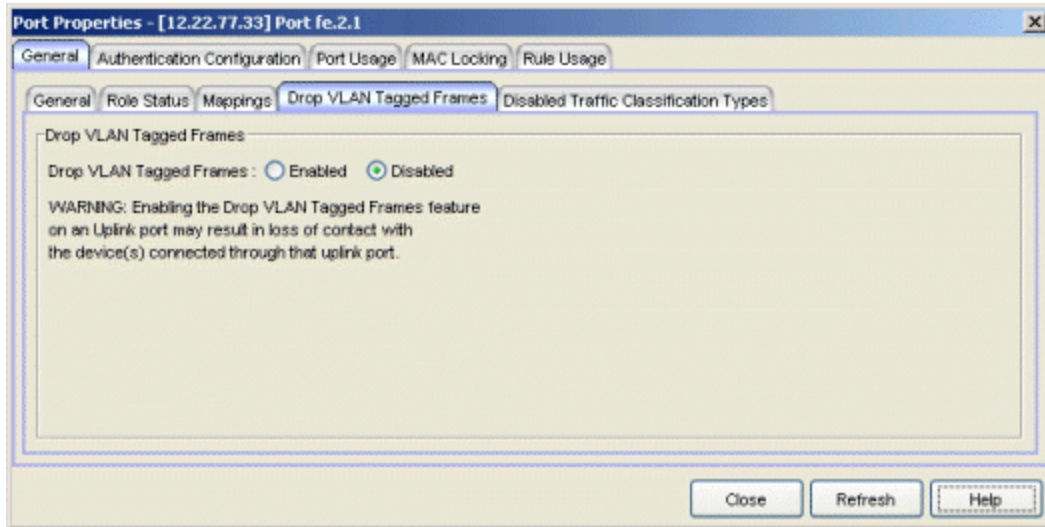
This tab lets you enable or disable the Drop VLAN Tagged Frames feature on this port. When the Drop VLAN Tagged Frames feature is enabled, any packet already tagged with a VLAN coming into the port will be dropped. This provides extra security in that it prevents users from, for example, coming in with a card capable of VLAN tagging and attempting to access the network. In most cases, you would enable this feature on user ports because you don't want users to be tagging their own traffic, and you would disable it on interswitch link ports, where you want tagged packets to be accepted.

It is recommended that you enable the Drop VLAN Tagged Frames feature when you set a default role on a port or when you enable authentication on a port, because these things indicate that the port is a user port that should not be transmitting tagged packets. You can enable Drop VLAN Tagged Frames for a single port here, or on multiple ports simultaneously using the [Port Configuration Wizard](#). If the device does not support Drop VLAN Tagged Frames, this tab is grayed out.

---

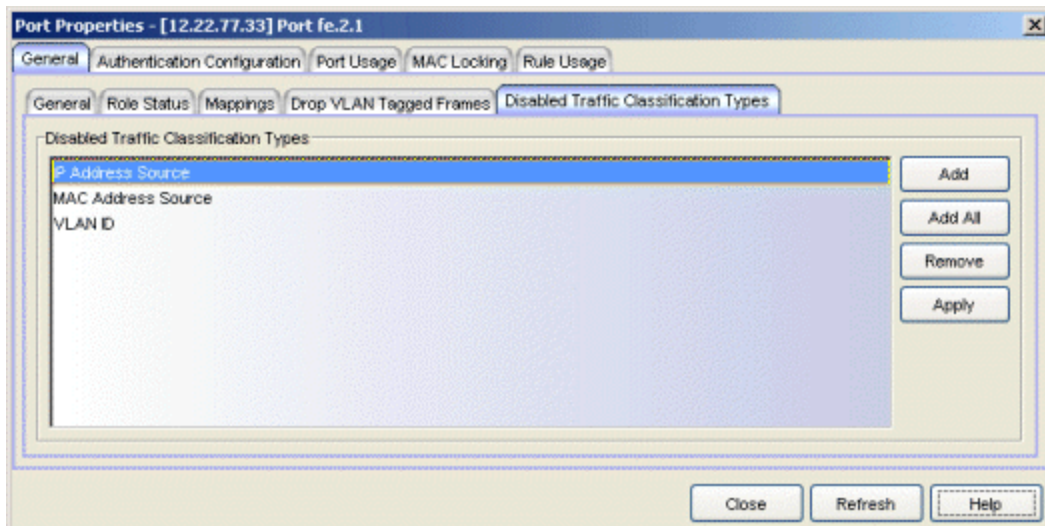
**WARNING:** Enabling this feature on an Interswitch or Backplane port is likely to result in loss of contact with devices connected through the port.

---



## Disabled Traffic Classification Types Tab

Use this tab to specify rule types that will be disabled on the port. You can disable specific classification rule types on an individual port as a way to disable policy-assignment rules used in VLAN to Role Mapping, IP to Role Mapping, MAC to Role Mapping, and Role Override. For example, you can disable the VLAN ID traffic classification type to disable Tagged Packet VLAN to Role Mapping on the port. You can also disable all traffic classification types, which effectively turns off policy on the port.



Use the Add or Add All button to create a list of rule types that will be disabled on the port.



### Add Button

Opens the [Traffic Classification Type wizard](#) where you can select the traffic classification type you want to disable on the port and add it to the list.

### Add All Button

Adds all traffic classification types to the list. This would disable all traffic classification on the port, and the role's default class of service and/or default access control would take effect.

### Remove Button

Removes the selected traffic classification type from the list.

### Apply Button

Applies the list of disabled traffic classification types to the port.

---

## Related Information

For information on related concepts:

- [Authentication](#)

For information on related tasks:

- [How to Configure Ports](#)
- [How to Freeze/Unfreeze a Port](#)

For information on related windows:

- [Port Properties - Authentication Configuration Tab](#)
- [Port Properties - Port Usage Tab](#)

## Port Properties MAC Locking Tab

---

The Port Properties MAC Locking tab lets you enable or disable the [MAC Locking](#) feature on the selected port, if the device supports it. You can also view and change a list of MAC addresses that are currently locked on the port.

There are two ways to access the MAC Locking tab:

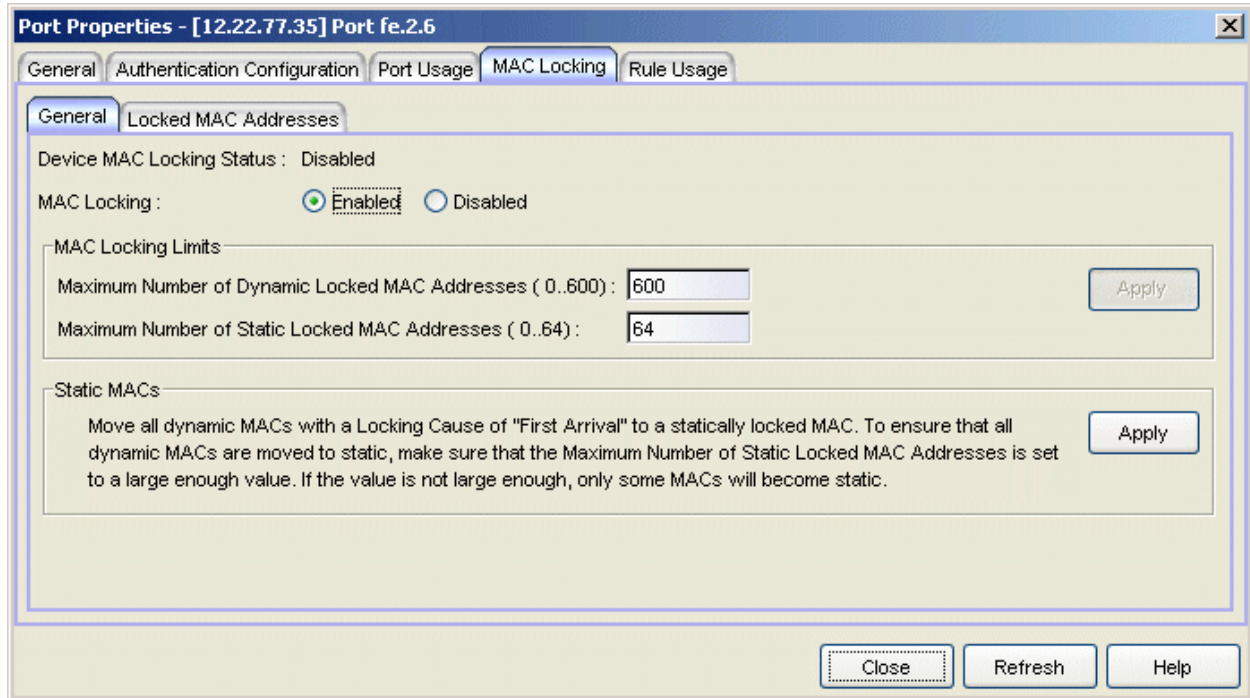
- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the MAC Locking tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the MAC Locking tab in the right panel.

In order for MAC Locking to take effect on a port, it must be enabled at the device level. You can do this using the [Device Configuration wizard](#), or the device [MAC Locking tab](#). You can also enable MAC Locking for selected ports in the [Port Configuration wizard](#). The MAC Locking tab provides two sub-tabs:

- [General Tab](#)
- [Locked MAC Addresses Tab](#)

### General Tab

This tab lets you enable/disable MAC Locking on the port as well as view the MAC locking status on the device. You can also set MAC locking limits and change all dynamic MACs (with a locking cause of "First Arrival") to statically locked MACs.



### Device MAC Locking Status

Shows whether the [MAC Locking](#) feature is enabled or disabled the device. If the device does not support MAC locking, this option is grayed out. In order for MAC Locking to take effect on a port, it must be enabled at the device level. You can do this using the device [MAC Locking tab](#).

### MAC Locking

Lets you to enable or disable the [MAC Locking](#) feature on this port. If the device does not support MAC locking, this option is grayed out.

### *MAC Locking Limits*

#### Maximum Number of Dynamic Locked MAC Addresses

Allows you to set the maximum number of MAC addresses that can be locked dynamically on the port. The numbers in parentheses let you know the range of allowed values for the particular device. When you enable Dynamic MAC Locking on a port, the next MAC address that authenticates or accesses the port (up to the maximum number of dynamic locked MAC addresses) will have exclusive access to that port from that time on. If you are using static locked MAC addresses, the maximum number of dynamic locked MAC addresses is usually set to 0.

### Maximum Number of Static Locked MAC Addresses

Allows you to set the maximum number of MAC addresses that can be locked administratively on the port. The numbers in parentheses let you know the range of allowed values for the particular device. Static MAC Locking lets you create a list of locked MAC addresses for a port so that the port only accepts traffic from those MAC addresses.

### Apply Button

Applies the MAC limits you've set.

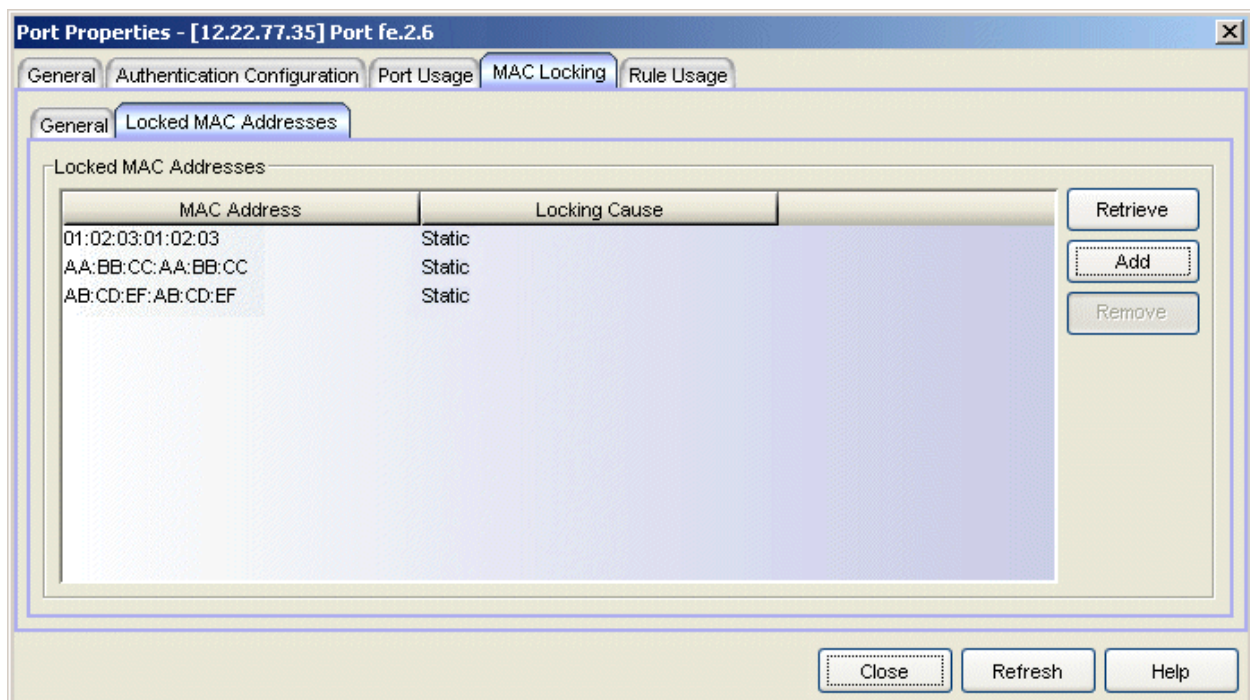
### Static MACs

#### Static MACs

Click **Apply** to change all Dynamic Locked MAC addresses (with the [Locking Cause](#) of "First Arrival") to Static Locked MAC addresses. To ensure that all Dynamic Locked MAC addresses are changed to Static, make sure that the [Maximum Number of Static Locked MAC Addresses](#) is set to a large enough value.

## Locked MAC Addresses Tab

This tab lets you view a list of the MAC addresses currently locked on the selected port. You must click the **Retrieve** button to display this information.



### MAC Address

MAC address that is locked.

### Locking Cause

Indicates why the MAC address is locked:

- **Authentication** - Locked as the result of authentication
- **First Arrival** - Locked because it was the first MAC address to access the port
- **Static** - MAC address was added to the list administratively

### Retrieve Button

Populates the Locked MAC Addresses table with a list of the MAC addresses currently locked on the selected port.

### Add Button

Opens the [Add Static MAC window](#), where you can create a list of locked MAC addresses for this port.

### Remove Button

Removes the selected entry from the Locked MAC Addresses table.

---

## Related Information

For information on related concepts:

- [MAC Locking](#)

For information on related tasks:

- [How to Configure Ports](#)

For information on related windows:

- [MAC Locking Tab \(Device\)](#)
- [MAC Locking Tab \(Device Group\)](#)
- [MAC Locking Tab \(Port Group\)](#)

## Port Properties Port Usage Tab

---

The Port Properties Port Usage tab displays information related to end user login ([authentication](#)) sessions, rate limit violations, and CEP (Convergence End Point) connections on a port.

There are two ways to access the Port Usage tab:

- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the Port Usage tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the Port Usage tab in the right panel.

The Port Usage tab provides four sub-tabs:

- [End User Sessions Tab](#)
- [End User Session Settings Tab](#)
- [Rate Limit Violations Tab](#)
- [CEP Usage Tab](#)

## End User Sessions Tab

This table displays information about login sessions for the port, 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. You must click **Retrieve** to display the port information in the table.

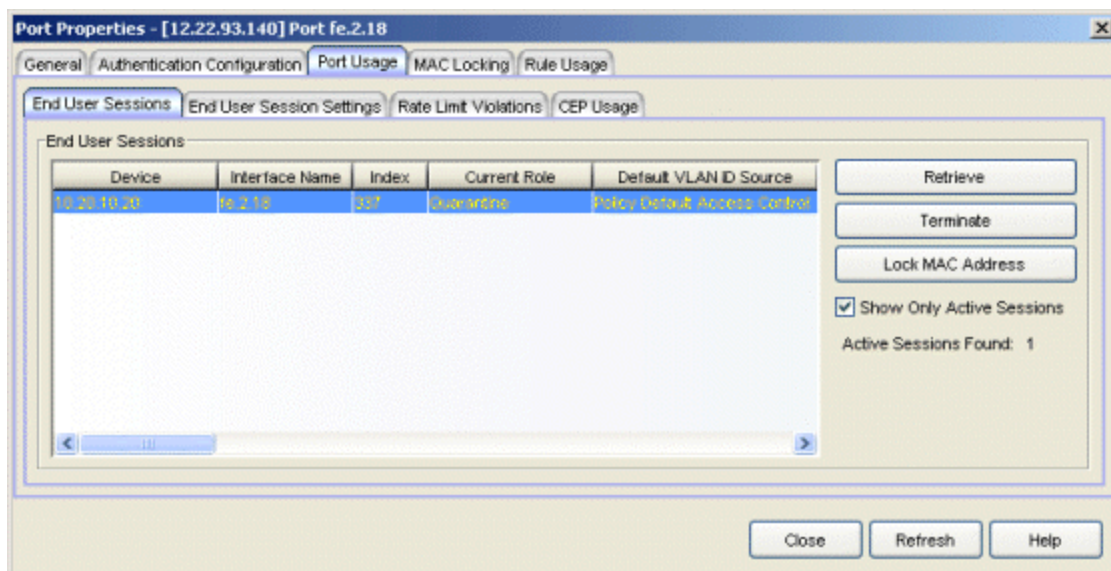
By default the **Show Only Active Sessions** checkbox is checked, and only your active sessions are displayed. Deselect the checkbox to display all entries. Active sessions that are being applied to traffic are listed in blue text. Active sessions that are not being applied are listed in green text. Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, and MAC all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type will be applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user

authentication enabled (802.1X, Web-Based, and MAC,) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

**NOTE:** Devices configured for multi-user authentication always list *only* active sessions even if the Show Only Active Session checkbox is deselected.

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port will show up in the table. For devices that support multiple authenticated users per port, all users authenticated on the port will be listed in the table, along with the roles under which they are authenticated.



### Device

The IP address or name of the device where the port is located.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### Alias

The alias (ifAlias) for the port interface, is one is assigned.

### Type

The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Auto Tracking, Quarantine, or Role Override. If Role Override is displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role. An example of this would be if the Automated Security Manager has detected a threat on the port, and used a MAC address rule to apply the Quarantine role to the end user.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

### MAC Address

The MAC address of the remote user of this login session.

### IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session. If Anti-Spoofing is enabled and configured, this column displays IP addresses found in the Anti-Spoofing MAC-to-IP address binding table. For more information, see [How to Configure Anti-Spoofing](#).

### Hostname

The hostname of the remote user of this login session. To determine the hostname, Policy Manager takes the IP address (when available) and uses the hostname cache on the NetSight server. The hostname cache must be explicitly enabled by selecting the "Enable Name Resolution" option in the Tools > Options > Suite Options > panel (by default, this option is disabled). Once the hostname cache is enabled, name resolution must be enabled for Port Usage tabs using the Tools > Options > Policy Manager > [Name Resolution \(PM\)](#) panel.

### Current Role

The role under which the user authenticated on the port. If a session displays "Invalid Role" in this column, check the Invalid Role Action setting on the [device Role/Rule tab](#) to see the action that was configured in the



event a user is assigned an unknown or invalid role. If the user authenticated via [RFC 3580 VLAN Authorization](#), this column will display the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been configured, the port's Default role will be displayed (if there is one); otherwise, the column will display "N/A."

### Default VLAN ID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

### Default VLAN ID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

### RFC3580 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."

### 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." Use the [Port Properties Authentication Configuration tab](#) to change these settings, if desired.

**Start Time**

The time and date when the login session started.

**Duration**

The duration of the user's login session, in the format D + HH:MM:SS.

**Authentication Status**

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

**Terminate Cause**

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed

- Unknown Termination Cause
- User Logged Out

### Authentication Server

The RADIUS server that authenticated the session.

### Session ID

A unique identifier for the session. For devices that support multiple authenticated users per port, each user on the port will have a different session ID. Sessions with an authentication type of MAC or [Role Override](#) will display "N/A."

### 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. Devices must be created using SNMPv3 in order to see this value. Devices using SNMPv1 will display "N/A."

### Transmitted Bytes

The number of bytes transmitted in user data frames on this port during this session. Devices must be created using SNMPv3 in order to see this value. Devices using SNMPv1 will display "N/A."

### Received Frames

The number of user data frames received on this port during this session.

### Transmitted Frames

The number of user data frames transmitted on this port during this session.

### Retrieve Button

Displays the latest information for the port.

### Terminate Button

Select an active session and click **Terminate** to end the session. If multiple sessions are selected, only active sessions will be terminated. You cannot terminate a session on a [frozen port](#) and you cannot terminate Role Override (IP) or Role Override (MAC) sessions that were created through the CLI (command line interface).

### Lock MAC Address Button

Enables [MAC Locking](#) on the selected port(s) (static MAC locking). MAC locking must be enabled on the device in order for it to be enabled on a

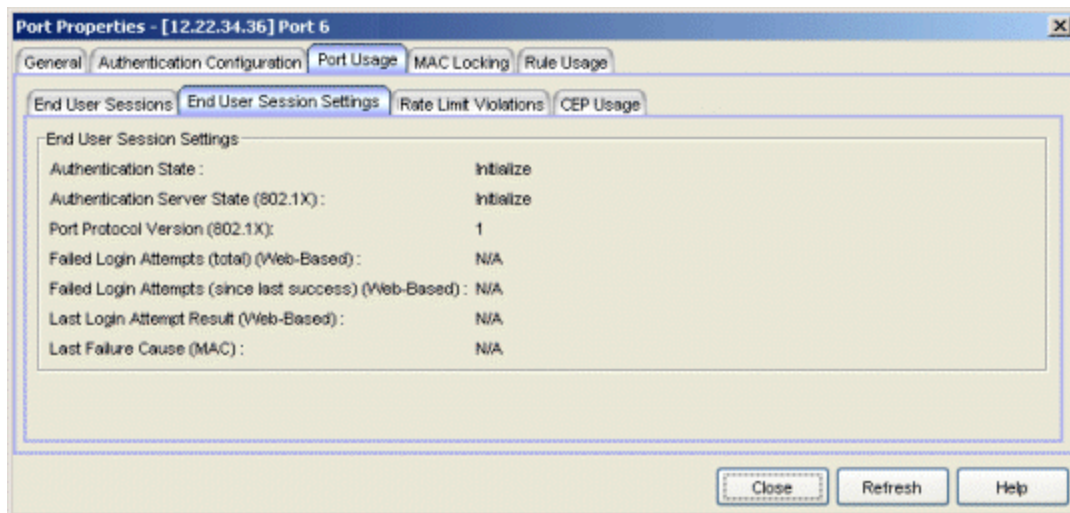
port.

### Show Only Active Sessions Checkbox

Select this checkbox to display only active sessions (listed in blue text) in the table.

## End User Session Settings Tab

This tab displays the current authentication state and login statistics for the port. Because this section displays information for a single end user login session, these fields are grayed out for devices that support multiple authenticated users per port.



### Authentication State

Current state of the port with regard to authentication. If "None," authentication is not enabled on the device.

For web-based authentication:

- **Disconnected** - There is no end user currently logged in on the port.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.

For 802.1X authentication:

- **Initialize** - The port is initializing. One reason for this is that the device has been reset.
- **Disconnected** - There is no end user currently logged in on the port.
- **Connecting** - The port is establishing communication with an end user.
- **Authenticating** - An end user is in the process of logging in and being authenticated.
- **Authenticated** - An end user is currently logged in and authenticated.
- **Aborting** - The authentication procedure is being prematurely terminated due to, for example, a re-authentication request or an authentication timeout.
- **Held** - The port is locked and authentication attempts are not allowed. Occurs when, for example, an end user tries to log in several times with an incorrect password.
- **Default Role** - An end user has connected and is using the port's default role. Occurs when the port mode is set to Inactive/Default (see [Port Mode](#) for more information).
- **No Authentication** - No end user can be authenticated because the port mode is set to Inactive/Discard (see [Port Mode](#) for more information).

---

**NOTE:** RoamAbout R2 devices always show "Authenticating" as their Authentication State. Because R2 devices can have multiple users authenticated to the same port, "Authenticating" simply denotes that the port is currently open for users to authenticate.

---

### Authentication Server State (802.1X)

For ports using 802.1X authentication, the current status of the authentication server, or the activity in which it is currently engaged.

- **Request** - A request for authentication has been received by the authentication server.
- **Response** - The authentication server is in the process of responding to an authentication request.
- **Success** - Authentication of the end user has succeeded.
- **Fail** - Authentication of the end user has failed.
- **Timeout** - The authentication attempt has timed out.

- **Idle** - The authentication server is ready to accept authentication requests, but no requests are currently being processed.
- **Initialize** - The authentication server is initializing. One reason for this is because the machine on which the server is located has been reset.

#### Port Protocol Version (802.1X)

For ports using 802.1X authentication, the protocol version number of the EAPOL (Extensible Authentication Protocol Over LANs) implementation supported by the port.

#### Failed Login Attempts (total) (Web-Based)

For ports using web-based authentication, the total number of failed login attempts on this port.

#### Failed Login Attempts (since last success) (Web-Based)

For ports using web-based authentication, the total number of failed login attempts since the last successful login on this port.

#### Last Login Attempt Result (Web-Based)

For ports using web-based authentication, indicates the result (success/failure) of the last attempt to log in to this port. Possible results are as follows:

- **Not logged in since last reset** - No login in since reset.
- **Authentication accepted** - User logged in successfully.
- **Authentication rejected**
  - Username or password mismatch
  - User misconfiguration (e.g. Deny Remote Permission in Active Directory Users).
- or, when two RADIUS servers are configured in the device:
  - Mismatched Shared Secret in a primary RADIUS server or both RADIUS servers.
  - Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown policy** - No policy (Role) defined in the device.
- **Unknown authentication server response** - When one RADIUS server is configured in the device:
  - Wrong Authentication UDP port number defined.
  - Mismatched Shared Secret.

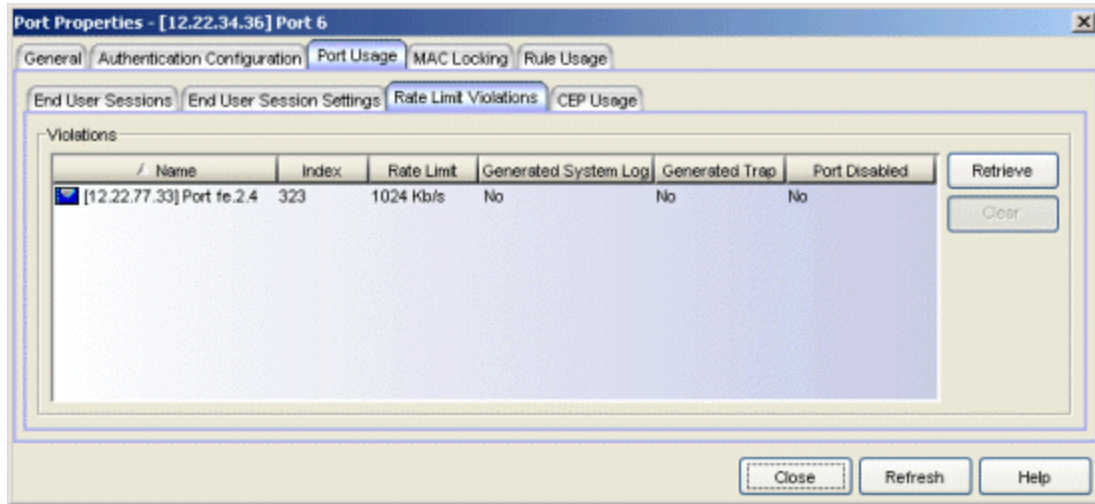
- RADIUS server is not contactable, or RADIUS server is down.
- Unsupported protocol (e.g. CHAP) configured on the device.
- **Unknown authentication client error** - User enters no username and password.
- **Auth client disabled or unavailable** - RADIUS server is disabled in the device.
- **Port authentication pending** - Port is in the process of authenticating.
- **Port held for too many failed attempts** - User reached the maximum number of failed attempts to log in.
- **Port held: Max attempts exceeded** - User exceeded the maximum number of failed attempts to log in once the port has been held.
- **Authentication server timeout** - When two RADIUS servers are configured in the device:
  - Wrong Authentication UDP port number defined in a primary RADIUS server or both RADIUS servers.
  - RADIUS servers are not contactable
  - Unsupported protocol (e.g. CHAP) configured on the device.

#### Last Failure Cause (MAC)

For ports using MAC authentication, the reason for the last authentication failure on the port.

## Rate Limit Violations Tab

This tab displays information about the rate limit violations for the port, including the current data being collected for a session in progress and data from previous sessions. You must click **Retrieve** to display the port information in the tables. For more information, see [Defining Rate Limits](#).

**Name**

The port interface name.

**Index**

The port index number.

**Rate Limit**

The rate limit that has been violated (exceeded).

**Generated System Log**

Indicates whether a syslog message was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

**Generated Trap**

Indicates whether an audit trap was generated when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

**Port Disabled**

Indicates whether the port was disabled when the rate limit was first exceeded. You can specify this action on a per-rate limit basis in the rate limit [General tab](#).

**Retrieve Button**

Retrieves the most recent rate limit violations information for the port.

**Clear Button**

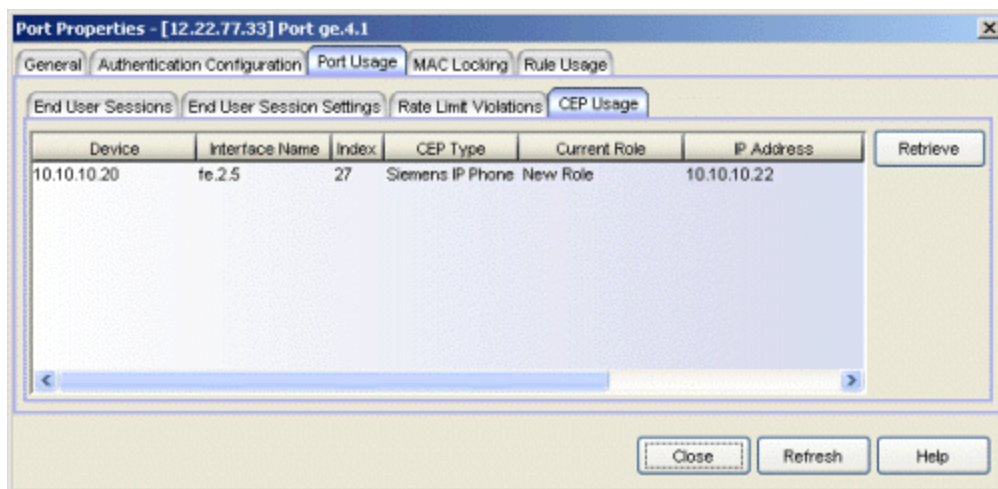
Clears the violations table. If port traffic continues to exceed the rate limit, the violations will reappear in the table.



## CEP Usage Tab

This tab displays information about each CEP connection for the ports on the device, including the date and time the connection was made. For devices that support one CEP connection per port, a connection entry remains in the table until a new connection is made on that port or the system is rebooted. You must click **Retrieve** to display the connection information in the table.

Refer to the [device Authentication tab \(CEP sub-tab\)](#) for information on enabling and configuring CEP on devices that support it.



### Device

The IP address or name of the device where the port is located.

### Interface Name

A description of the port.

### Index

The index value assigned to the port interface.

### CEP Type

The CEP product type that has made the connection.

### Current Role

The assigned role for the CEP connection. Each CEP product type has a role mapped to it. When a CEP connects to the network, the device identifies the CEP type and applies the assigned role. You can map a role for a CEP using the [device Authentication tab \(CEP sub-tab\)](#).

### IP Address

The IP address of the CEP connecting to the port.

**MAC Address**

The MAC address of the CEP connecting to the port.

**Start Time**

The date and time the connection was made.

**Retrieve Button**

Gets the port's CEP connection information and displays it in the table.

---

**Related Information**

For information on related concepts:

- [Authentication](#)
- [MAC Locking](#)
- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Ports](#)
- [Authentication Configuration Guide](#)
- [Defining Rate Limits](#)

For information on related windows:

- [Port Properties - Authentication Configuration Tab](#)
- [Port Properties - General Tab](#)
- [General Tab \(Rate Limit\)](#)

## Port Properties Rule Usage Tab

---

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. The Port Properties Rule Usage tab displays all the rules that have been used on the selected port, and the role they are associated with.

There are two ways to access the Rule Usage tab:

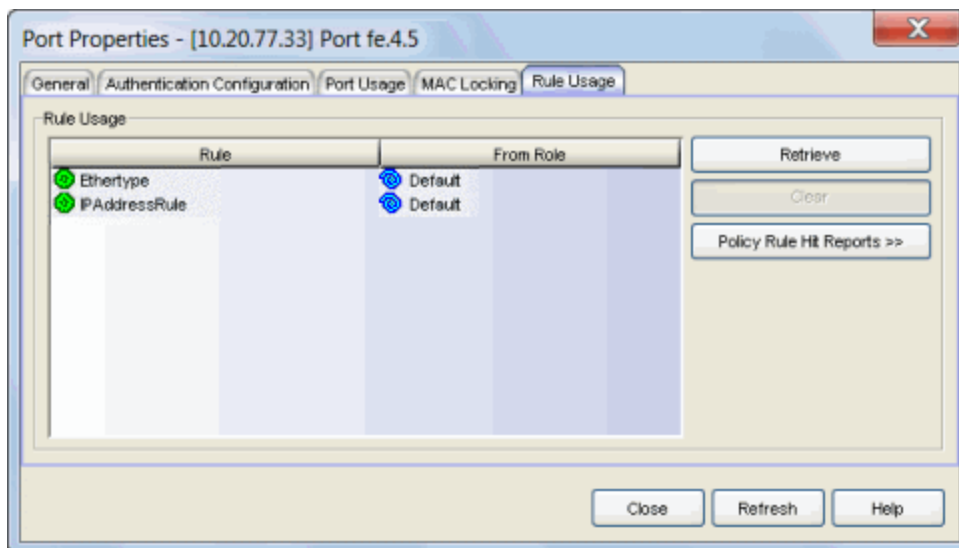
- Select a device in the left-panel Network Elements tab. In the right-panel Ports tab, select a port and click the Port Properties button. In the Port Properties window, select the Rule Usage tab (in the top row of tabs).
- Select a port in the left-panel Port Groups tab, then select the Rule Usage tab in the right panel.

Click the **Retrieve** button to display the rule usage information. Rule accounting must be enabled on the device; see the [device Role/Rule tab](#) for information.

---

**TIP:** You can see rule accounting information for an individual rule using the [Rule Usage Tab \(Rule\)](#).

---



### Rule

The name of the rule used on the port.

### From Role

The role that the rule is associated with.

### Retrieve Button

Retrieves/updates the rule usage information.

### Clear Button

Clears the port from the selected rule's usage list.

### Policy Rule Hit Reports

Select a port and use this button to access two [Policy Rule Hit Reports](#):

- Policy Rule Hits - this report shows the last 100 rule hits for the selected port.
- Top-5 Rule Usage Trend (1 week) - this report shows the top five rules with the most rule hits based on the last 7-day period for the selected port.

---

### Related Information

For information on related tasks:

- [How to Create or Modify a Rule](#)
- [How to Configure Devices](#)

For information on related windows:

- [Role/Rule Tab \(Device\)](#)
- [Rule Usage Tab \(Rule\)](#)

## Pre-Defined Well-Known IDs Window

---

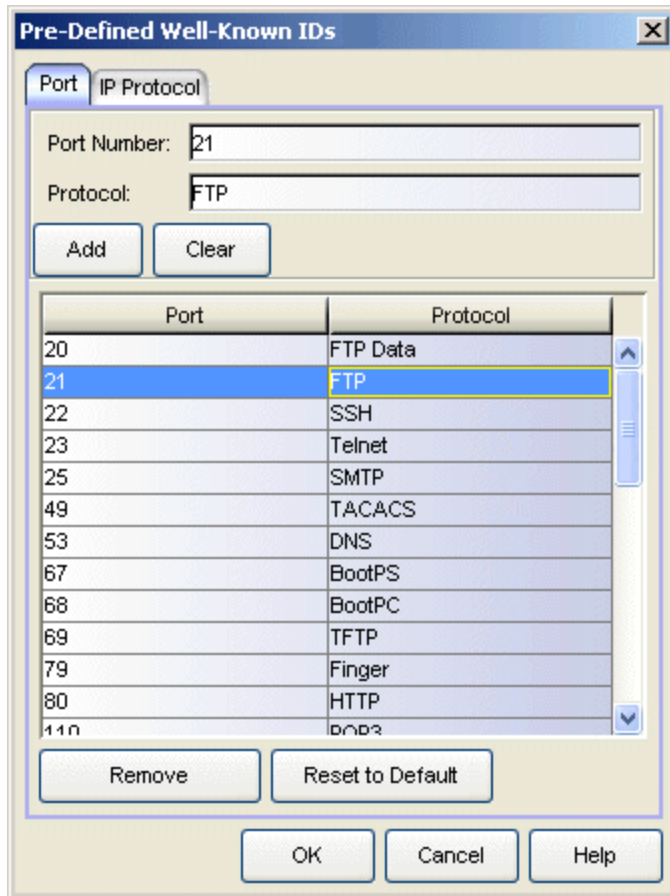
This window lets you add to the pre-defined list of well-known identifiers (IDs) used when creating Policy Manager rules. You can define a new ID for a TCP/UDP port number (Layer 4 Application Transport traffic classification type) or for an IP Protocol Type (Layer 3 Network traffic classification type). Once defined, these IDs are available for selection from the list of well-known values when defining the rule's traffic classification type.

To access the window, select **Edit > Pre-Defined Well-Known IDs** from the menu bar. IDs are defined using either of two tabs:

- [Port Tab](#)
- [IP Protocol Tab](#)

### Port Tab

The Port tab lets you define an ID for a TCP/UDP port number. Once defined, this ID can be used when creating a Policy Manager rule with a Layer 4 Application Transport traffic classification type.



### 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

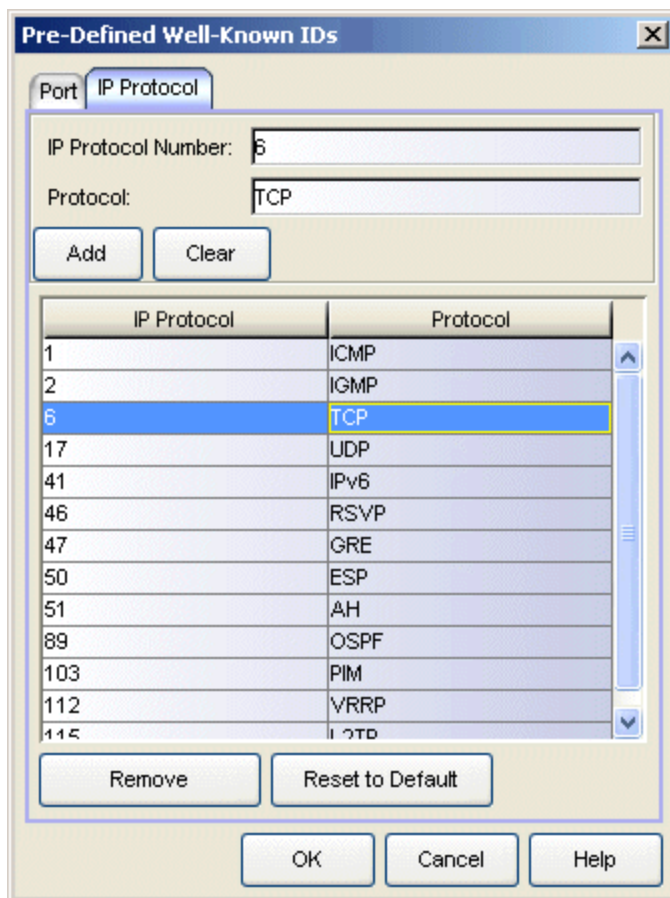
Deletes the selected ID(s) from the list of well-known IDs.

**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 a Policy Manager rule with a Layer 3 Network Traffic Classification Type.

**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 concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Define Well-Known IDs](#)
- [How to Create or Modify a Rule](#)



## Role/Service Usage Window

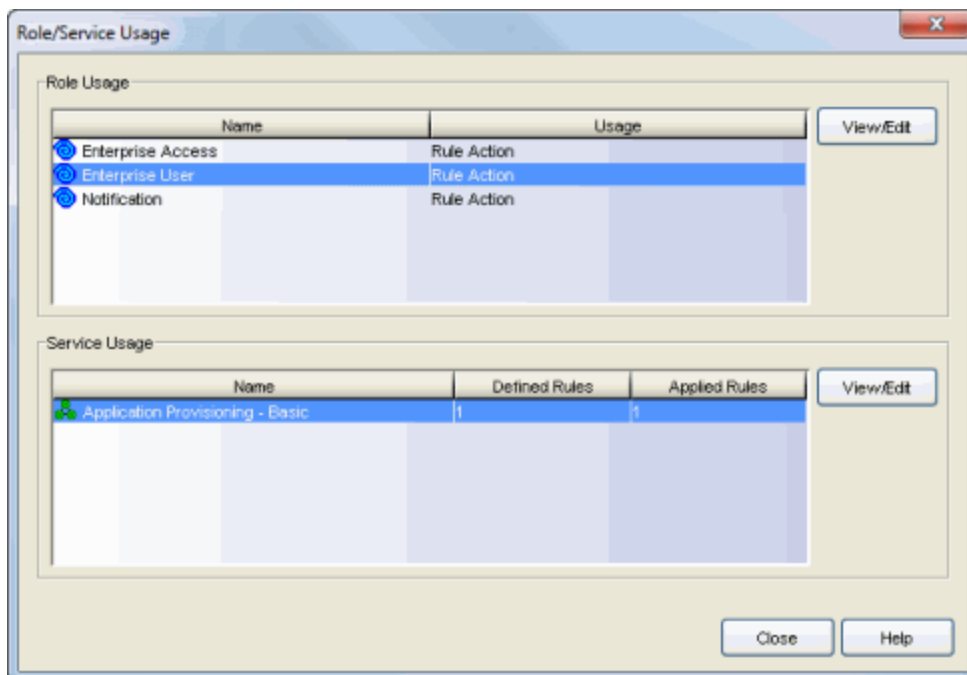
---

This window displays a list of roles and/or services that are using the Quarantine role, Class of Service (CoS) component, or VLAN you have selected.

To access this window for a Quarantine role, select the  button from the top right of the role's General tab.

To access this window for a CoS component or VLAN, right-click on a CoS component in the Class of Service Configuration window or a VLAN in the Access Control Configuration window and select Role/Service Usage from the menu.

You can view and/or edit a role or service using the **View/Edit** buttons. Select a role or service in the table and click the button to open the left-panel Roles/Services tab with the role or service selected. You can then view and/or edit information in the right-panel tabs. If you make a change to the role or service, you will need to enforce it using the **Enforce** toolbar button.



---

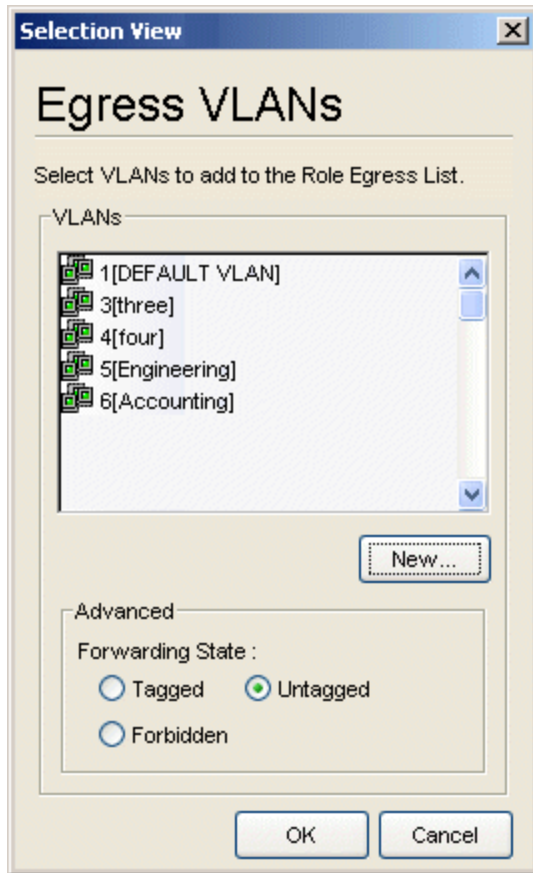
### Related Information

For information on related tasks:

- [Role General Tab](#)
- [Getting Started with Class of Service](#)
- [How to Create a VLAN](#)

## Selection View (Egress VLANs)

The Egress VLANs Selection View appears when you click the **Add** button in the VLAN Egress window in the [Role Wizard](#) or the role's [VLAN Egress tab](#). It allows you to add a VLAN to the Role's Egress list and specify the egress forwarding state.



### VLANs

This is a list of the available VLANs. Make a selection from this list, or click **New** to create a new VLAN and add it to the list.

### Forwarding State

Select the desired forwarding state: Tagged (frames will be forwarded as tagged), Untagged (frames will be forwarded as untagged), or Forbidden (frames will not be forwarded; they will be discarded).

### New Button

Opens the [Create VLAN Window](#), where you can create a new VLAN. The Create VLAN window returns you to the Selection View window after the VLAN has been created, and the new VLAN is available for selection in the list.

---

### Related Information

For information on related tasks:

- [How to Create a VLAN](#)

For information on related windows:

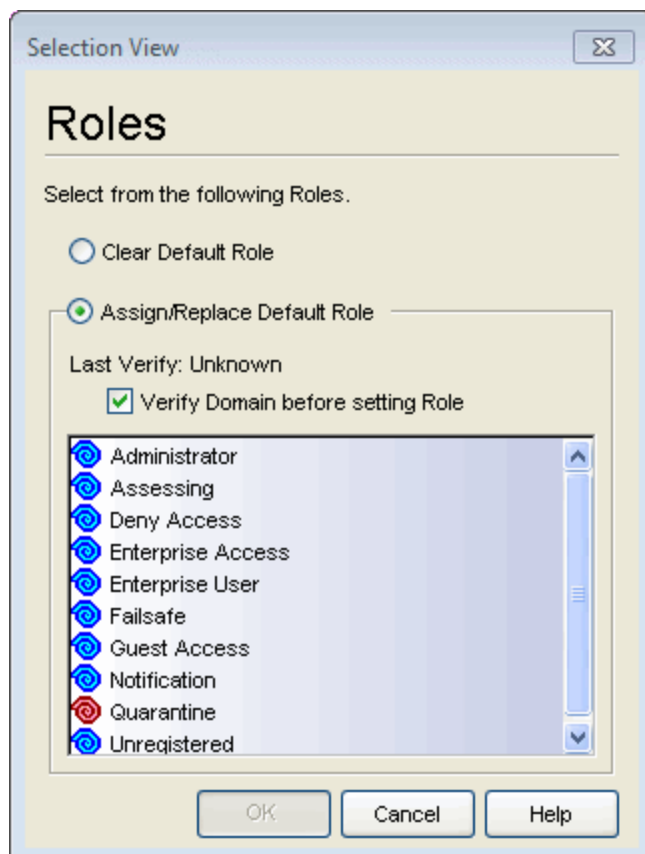
- [Create VLAN Window](#)
- [VLAN Egress Tab \(Role\)](#)

## Selection View (Roles)

---

The Roles Selection View appears in various instances:

- When you are selecting a [default role](#) for a port or a device. It also lets you clear the current default role from a port or device. To access this view, right-click the desired port or device in the left-panel Network Elements tab, then select Set Default Role from the menu. This view is shown below.
- When you are selecting a device-level role for a Matrix C1 device. To access this view, select the desired C1 device in the left-panel Network Elements tab, then click the **Select** button in the device's [Role/Rule tab](#).
- When you are selecting a role for VLAN to role mapping. It also lets you clear the current VLAN to role mapping. To access this view, click the desired VLAN in the left panel of the Access Control Configuration window (available from the Policy Manager Edit menu), then click the **Select** button in the VLAN to Role Mapping section on the VLAN's [General tab](#).



**Clear Default Role**

Select this option to clear the current role selection.

**Assign/Replace Default Role**

Select this option to assign a new role and make a selection from the list of available roles.

**Verify Domain before setting Role**

Select this option to verify the domain before setting a default role.

Deselecting the option allows the default role to be set without confirming that the domain configuration is in sync with the device or devices. Verify can be time consuming, so this option lets you skip it if you are confident that the device has the expected configuration. If in doubt, you should set the option to verify the domain. Above the checkbox you will see previous Verify information that will help you determine whether you should verify or not.

---

**Related Information**

For information on related tasks:

- [Creating a Role Using the Role Wizard](#)

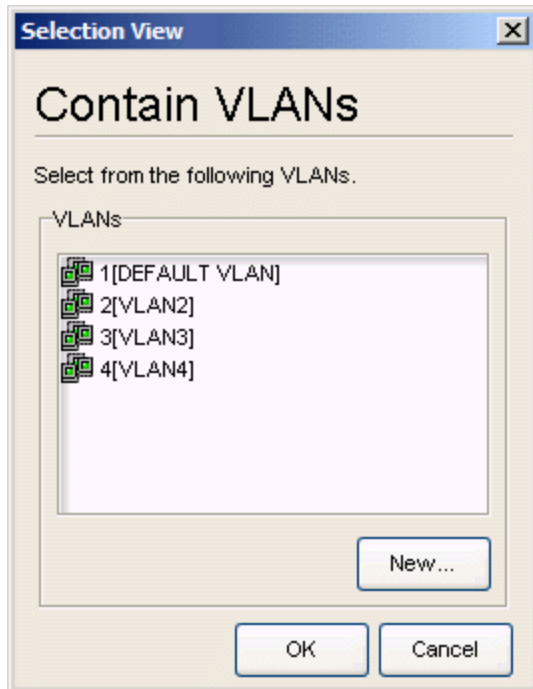
For information on related windows:

- [Port Properties - General Tab](#)
- [Role/Rule Tab \(Device\)](#)
- [General Tab \(VLAN\)](#)

## Selection View (VLANs)

---

This window appears when you click the **Add** button when configuring Authentication-based or Tagged Packet VLAN to Role Mapping in the [Role wizard](#) or the role's [Mappings tab](#). The Selection View lists all VLANs and allows you to select from the list to add to the role's VLAN mapping table.



### VLANs

Make a selection from the list of VLANs, or click **New** to create a new VLAN and add it to the list.

### New Button

Opens the [Create VLAN Window](#), where you can create a new VLAN. The Create VLAN window returns you to the Selection View window after the VLAN has been created, and the new VLAN is available for selection on the list.

---

## Related Information

For information on related tasks:

- [How to Create a VLAN](#)

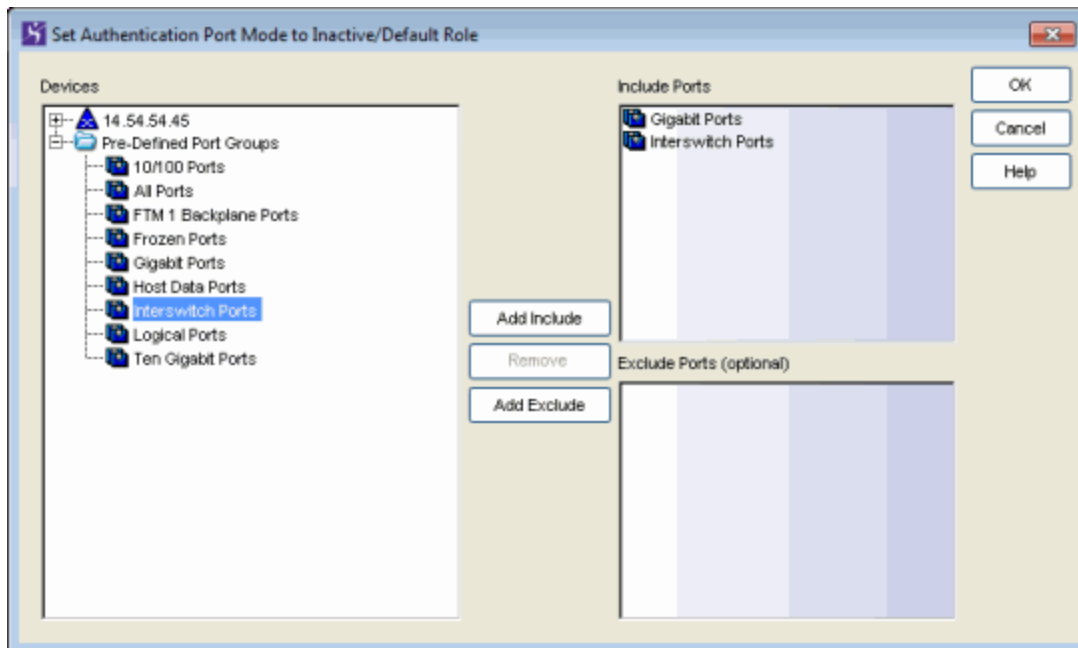
For information on related windows:

- [General Tab \(Rule\)](#)
- [Create VLAN Window](#)
- [General Tab \(Role\)](#)



## Set Authentication Port Mode to Inactive/Default Role Window

This window lets you select the ports you want to set to Inactive/ Default Role, prior to enabling authentication on a device. It is displayed when you select the **Select Ports to set to Inactive/Default Role** option on the Authentication Status window that appears when you elect to enable authentication in the [Device Configuration Wizard](#) or on the device [Authentication tab](#).



### Devices

Lists the ports and port groups you can [select](#) for addition to the Include Ports and Exclude Ports lists. To add a port or port group, select it and click **Add Include** or **Add Exclude**.

### Include Ports

Lists the ports and port groups you want to be changed to Inactive/Default Role. To add a port or port group to this list, [select](#) it and click **Add Include**. To remove a port or port group from the list, select it and click **Remove**.

### Exclude Ports

Lists the ports and port groups you don't want changed to Inactive/Default Role. It is not necessary to add all the ports and port groups you don't want changed to this list. Simply leaving them off the Include Ports list means

they won't be changed. However, the Exclude Ports list enables you to, for example, add the All Ports port group to the Include Ports list, but add the Interswitch Ports port group to the Exclude Ports list so all but the interswitch ports will be changed. To add a port or port group to this list, [select](#) it and click **Add Exclude**. To remove a port or port group from the list, select it and click **Remove**.

#### **Add Include Button**

Adds the ports or port groups selected in the Devices list to the Include Ports list.

#### **Remove Button**

Removes the selected ports or port groups from the Include or Exclude Ports List.

#### **Add Exclude Button**

Adds the ports or port groups selected in the Devices list to the Exclude Ports list.

---

### **Related Information**

For information on related tasks:

- [How to Configure Devices](#)

For information on related windows:

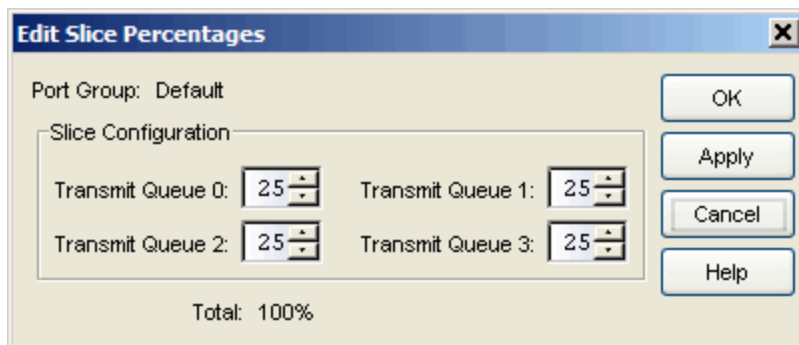
- [Authentication Tab \(Device\)](#)

## Slice Percentages Window

This window lets you configure the slice percentages for each transmit queue. These percentages are used when configuring the weighted fair queuing arbiter mode for a transmit queue port group. They determine the way that traffic in each queue will be serviced. (For more information on the arbiter mode, see [Transmit Queue Bandwidth Configuration](#).) The number of transmit queues varies by port type. The graphic below shows an Edit Slice Percentages window for a 4-queue port type.

To access this window, open the Class of Service Configuration window (available from the Policy Manager Edit menu). Right-click on a value in the Transmit Queue Bandwidth column to open the Edit Bandwidth Configuration window. Select the Weighted Fair Queuing arbiter mode and then click the **Edit** button in the Slice Configuration section.

If you have configured multiple transmit queue port groups, you must use advanced mode to configure arbiter mode for the multiple groups. For more information, see the [Arbiter Mode tab](#) Help topic.



### Port Group

The port group whose slice percentages are being configured. Typically, this is the Default port group. However, for Advanced Mode, this is the transmit queue port group selected in the left-panel Classes of Service tree.

### Slice Configuration

Select the slice percentage to assign to each transmit queue. Percentages must add up to 100%. Configuring 100% for the highest priority (highest numbered) queue sets the arbiter mode to Strict mode.

## Related Information

For information on related concepts:

- [Getting Started with Class of Service](#)

For information on related tasks:

- [How to Configure Transmit Queues](#)

For information on related windows:


- [Arbiter Mode Tab \(Transmit Queue Port Group\)](#)

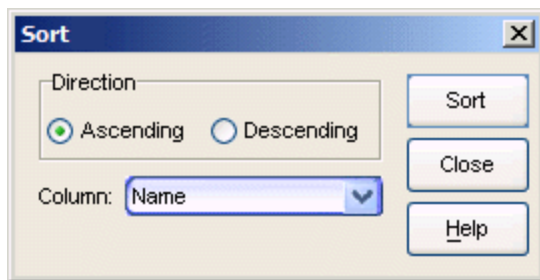
## Sort Window

---

The Sort window lets you sort column entries in the right panel in ascending or descending order. Text entries are sorted alphabetically, numeric entries are sorted numerically, and mixed entries are sorted alpha-numerically.

You can access the Sort window by selecting **View > Sort**. You can also sort a column by right-clicking on a column header and selecting **Sort Ascending** or **Sort Descending**.

**NOTE:** Some Policy Manager tables use a set of Table Tools to find, filter, sort, print, and export information in a table. You can access these Table Tools by clicking the Table Tools  button in the upper left corner of the table. For more information, see Table Tools.



### Ascending

Sorts the selected column in ascending order.

### Descending

Sorts the selected column in descending order.

### Column

Enables you to select the column to be sorted from a drop-down list.

### Sort Button

Performs the sort operation.

### Close Button

Exits the Sort window.

### Help Button

Displays detailed information about the current window.

## Related Information

For information on related tasks:

- [How to Filter, Find, and Sort](#)

## ToS/DSCP Configuration Window

---

The ToS/DSCP Configuration window allows you to configure a ToS (Type of Service) or DSCP (Diffserv Codepoint) value to automatically generate a hexadecimal number between 0 and FF. 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. (For an explanation of the ToS/DSCP field and the service parameters, see [IP Type of Service](#).)

In Policy Manager, you can configure a ToS/DSCP value in two different situations, as follows:

### IP Type of Service Classification

An IP Type of Service classification rule causes the one-byte ToS/DSCP field in the IP header of incoming packets to be read. If a value is found in this field and it matches the ToS/DSCP value specified in the classification rule, the packet is classified accordingly. You can access the ToS/DSCP Configuration window during the creation of the classification rule by clicking the **Select** button in the [Rule Wizard](#)'s or [Traffic Description Wizard](#)'s IP Type of Service window.

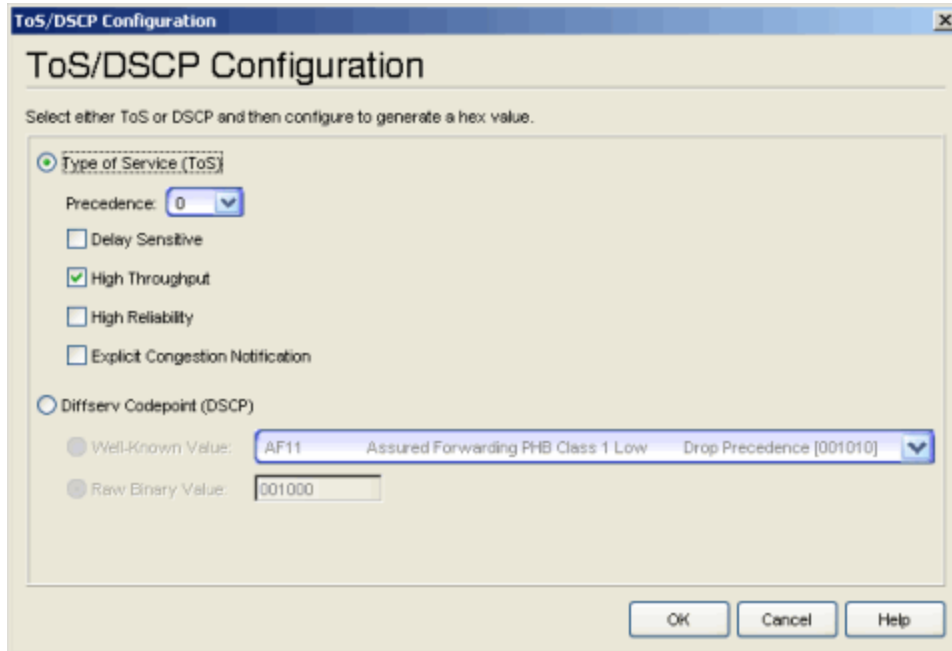
### ToS/DSCP Rewrite

Some IP rules allow a ToS/DSCP value to be written to the ToS/DSCP field in the IP header of incoming packets. If the packet's ToS/DSCP field is blank, the value specified in the rule is entered, or if the value is already present, it is replaced with the new value. The traffic is then classified accordingly. In Policy Manager, you specify the ToS/DSCP rewrite value by creating a CoS (class of service) and associating the appropriate ToS/DSCP value with it. You then select this CoS action for the classification rule. You can access the ToS/DSCP Configuration window during the creation of the class of service by clicking the **Select** button in the ToS section of the [Create Class of Service window](#) or the Class of Service [General tab](#). You then select this CoS action for the classification rule in the [Rule Wizard](#) or on the rule's [General tab](#).

---

**NOTE:** The ToS/DSCP Rewrite feature works only for the appropriate classification rules. It does not work at the role level. If you select a CoS that is associated with a ToS/DSCP value as the default CoS for a role, the ToS/DSCP value will be ignored.

---



### Type of Service (ToS)

Select this option to generate a ToS hexadecimal value.

### Precedence

Use the drop-down list to select the desired precedence. Precedence specifies the importance or priority of the traffic.

- 0 -- Routine
- 1 -- Priority
- 2 -- Immediate
- 3 -- Flash
- 4 -- Flash Override
- 5 -- CRITIC/ECP
- 6 -- Internetwork Control
- 7 -- Network Control

The Internetwork Control designation is intended for use by gateway originators only. The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network.

### Delay Sensitive

Select this check box to generate a Low Delay service parameter that will minimize delay.



### High Throughput

Select this check box to generate a High Throughput service parameter that will maximize throughput.

### High Reliability

Select this check box to generate a High Reliability service parameter that will maximize reliability.

### Explicit Congestion Notification

Select this check box to generate an Explicit Congestion Notification service parameter that will minimize monetary cost.

### Diffserv Codepoint (DSCP)

Select this option and use one of the Value fields to generate a DSCP hexadecimal value.

### Well-Known Value

The drop-down list presents recommended codepoints for three Differentiated Services (DS) Per-Hop-Behavior (PHB) groups called Assured Forwarding (AF), Class-Selector (CS), and Expedited Forwarding (EF). For more information on these PHB groups, refer to RFC 2474, RFC 2597 and RFC 2598.

### Raw Binary Value

Enter the raw DSCP binary value (a 6-bit value).

---

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)
- [ToS/DSCP Value Definition Chart](#)

For information on related tasks:

- [How to Create or Modify a Rule](#)

For information on related tabs:

- [General Tab \(Rule\)](#)

## Traffic Classification Type Wizard

---

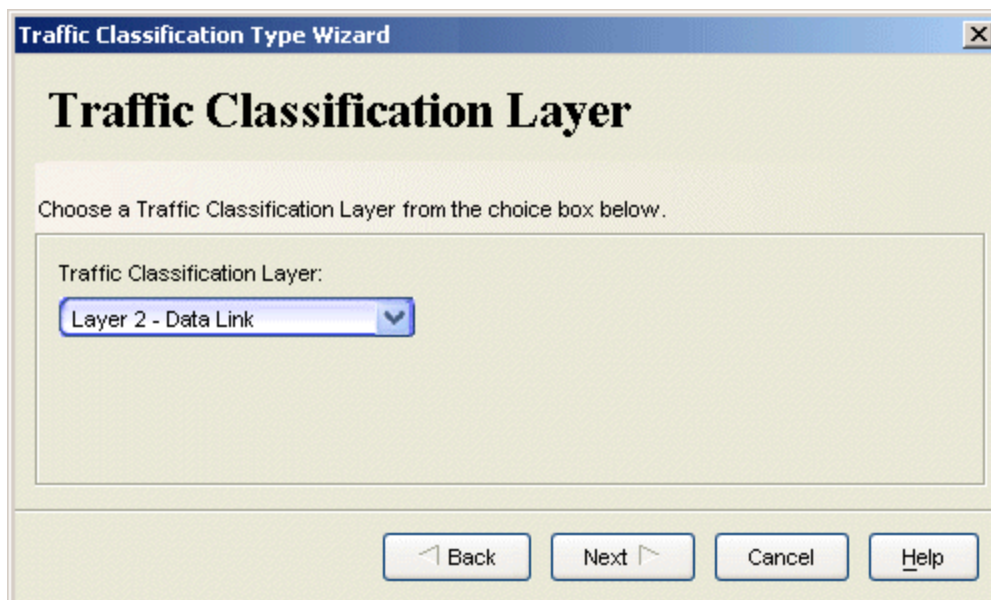
You can disable specific classification rule types on an individual port as a way to disable policy-assignment rules used in VLAN to Role Mapping, IP to Role Mapping, MAC to Role Mapping, and Role Override. For example, you can disable the VLAN ID traffic classification type to disable Tagged Packet VLAN to Role Mapping on this port.

The Traffic Classification Type Wizard lets you easily choose a rule type that you want to disable on the selected port. You choose the rule type by first selecting the traffic classification layer and then the classification type. For more information on traffic classification types, see [Traffic Classification Rules](#).

The Traffic Classification Type Wizard is accessed from the **Add** button in the Disabled Traffic Classification Type tab in the [Port Properties General tab](#).

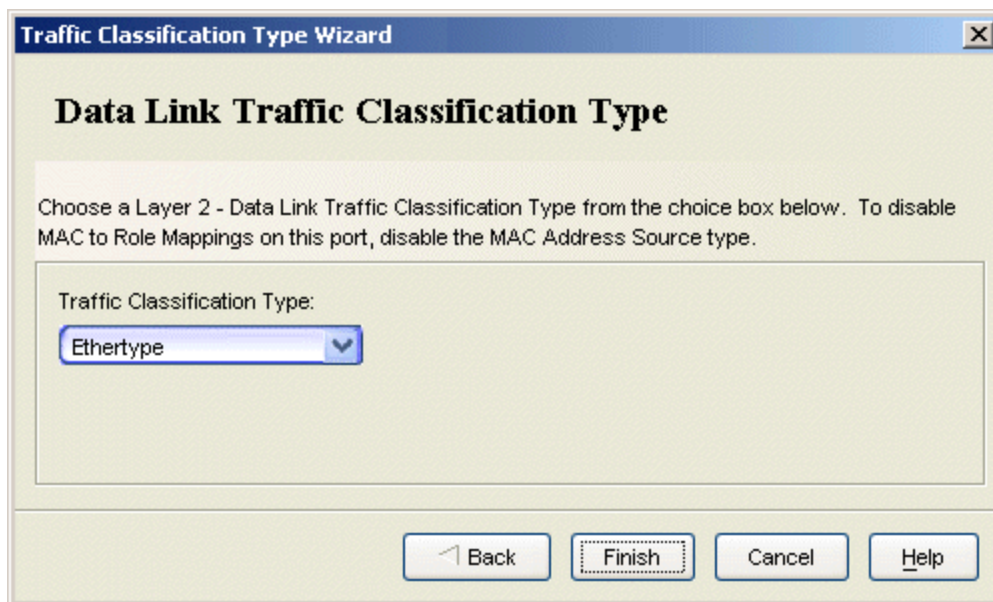
### Traffic Classification Layer

Use the drop-down list in this window to select the desired traffic classification layer. Classification types are grouped according to Layers 2, 3, and 4 of the OSI model: Data Link, Network, and Transport, respectively.



## Traffic Classification Type

Use the drop-down list in this window to select the desired traffic classification type. There are multiple classification types for each layer. The layer you selected in the previous window determines which types will be listed here.



### Finish Button

Click **Finish** to display the selected rule type in the Disabled Traffic Classification Type tab of the [Port Properties General tab](#).

## Related Information

For information on related concepts:

- [Traffic Classification Rules](#)

For information on related tasks:

- [How to Create a Rule](#)
- [How to Configure Ports](#)

For information on related tabs:

- [Port Properties General Tab](#)