Extreme Networks Extreme Management Center®

Automated Security Manager User Guide

Legal Notices

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

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

Trademarks

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

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

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

Support

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

Contact

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

Toll-free: +1 888-257-3000

Extreme Networks® Software License Agreement

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

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

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

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

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

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

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

7. TITLE AND PROPRIETARY RIGHTS

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

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

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

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

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

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

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

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

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

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in

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

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

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

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.

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

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

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

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

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

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

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

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

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

Table of Contents

Extreme Management Center® Automated Security Manager Help

Automated Security Manager (ASM) provides security management functionality that uniquely captures event information from multiple sources, resolves the threat to a specific user and switch/port, then implements the predetermined quarantine and remediation actions.

It combines the features of a comprehensive intrusion detection system, such as Extreme Networks Intrusion Prevention System (IPS), with NetSight Compass' search capabilities and NetSight Policy Manager to provide an effective defense against threats to the security of your network. In addition, Automated Security Manager lets you easily configure your responses to threats.

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

Automated Security Manager Overview

Following is an overview of how ASM defends your network against security threats:

- The IPS detects a security event and notifies ASM of end stations that are the source of threats on the network. Security events containing information about the threat (category, etc.) and the end station IP addresses are sent via an SNMPv3 trap (inform) with AuthPriv enabled. (The use of SNMPv3 with AuthPriv enabled provides a measure of security to minimize the chances of a malicious user sending traps to the Automated Security Manager and disabling the network.)
- ASM's search capability determines the switch and port.
- ASM then determines what action should be taken and applies the action on the port (no action, disable port, or apply a quarantine policy[1]).
- Finally, ASM notifies the IPS of the actions taken via an SNMPv3 trap (inform)[2].

[1] Requires NetSight Policy Manager to be installed.
[2] Requires the IPS to support receiving SNMPv3 traps (informs).

Document Version

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

Date	Revision Number	Description
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: 9034977-01

ASM Configuration Considerations

Review the following configuration considerations when installing and configuring NetSight Automated Security Manager (ASM).

CDP Implementation

CDP must be disabled on the downstream devices when attached to a device using multi-user authentication (such as the Matrix N-Series Platinum). ASM (by design) excludes CDP ports from responding to a threat. If a device using multi-user authentication has a downstream device attached, such as a RoamAbout R2 that is running CDP, then ASM is not able to respond to threats from the port to which it is attached.

Use NetSight Console's **CDP Status** FlexView to disable CDP on downstream devices.

For example, from Console:

1. Select the **Wireless** Device Group in Console's left (tree) panel.
2. Open the **CDP Status** FlexView in the right panel.
3. Select all rows and use the Table Editor to set the **Global Status** to *disable* for all devices.

Devices/Firmware that do not support CDP

Product Family	Firmware Version
EOS C2	1.00.20
Vertical Horizon	
VH-2402S	2.05.19
VH-2402-L3	1.00.16
VH-4802	2.05.05
VH-8TX1UM	2.04.07.08

Optimized Node/Alias Implementation

Automated Security Manager processes Extreme Networks IPS events by locating the intruder IP address stored in the event and then taking action. Devices implementing the *"optimized" Node/Alias MIB table* complete this search process far more quickly. The following table lists devices and firmware revisions supporting the optimized Node/Alias MIB table.

Devices/Firmware that support "Optimized" Node/Alias:

Product Family	Firmware Version
E1	3.00.xx 3.01.xx 3.02.xx
E6/E7 *(2nd/3rd Generation)*	5.06.xx 5.07.xx 5.08.xx
N3/N7 ***Platinum and Gold***	3.00.xx 4.00.xx 4.05.xx 4.11.xx
V2	2.03.xx 2.04.xx

Support for Optimized Node/Alias -- The Automated Security Manager Incident Detail view (right-click an entry in the Activity Monitor and select View Details) indicates whether a device supports the optimized Node/Alias table or not:

- "Reading ctAliasTable" means that the device does not support the optimized Node/Alias table.
- "Reading ctAliasProtocolAddressTable" means that the device does support the optimized Node/Alias table.

Devices that do not support Node/Alias:
-- Matrix C1
-- Matrix E5
-- Matrix E1 (1G6xx-xx)
-- Vertical Horizon
-- AP 3000
-- RoamAbout R2

These devices do not support any form of Node/Alias. For these devices, the Automated Security Manager search resolves the searched IP address to the corresponding MAC address and does a MAC-based search to locate the physical port. Routers must be included in the search scope in order to provide access to the routers' ARP cache. In addition, you must select the ipRouteTable and ipCIDRRouteTable MIBs in the Automated Security Manager Options MIB Selection panel.

Disable Node/Alias Learning -- Ensure that inter-switch links are not learning Node/Alias information, as it slows down searches and gives inaccurate results. Enabling CDP on inter-switch links disables Node/Alias learning. You can also disable Node/Alias learning on a switch port by setting the maximum number of entries per interface (*ctAliasConfigurationInterfaceMaxEntries*) to 0 on that port, using the Node Alias Control FlexView in Console.

The following table provides Automated Security Manager search time comparisons between optimized and not optimized Node/Alias implementations.

Search Time Comparisons:

Number of Devices	**Node/Alias Optimized 4000 entries**	**Node/Alias Not Optimized 4000 entries**	**Node/Alias Optimized 200 entries**	**Node/Alias Not Optimized 200 entries**
25	3 sec	1 min 40 sec	3 sec	7 sec
100	9 sec	5 min 50 sec	9 sec	25 sec
200	20 sec	11 min 10 sec	20 sec	47 sec
300	25 sec	16 min 52 sec	25 sec	1 min 13 sec
800	1 min 3 sec	58 min 46 sec	1 min 3 sec	3 min 13 sec

Getting Started with ASM

This Getting Started help topic takes you through the basic steps needed to configure the Extreme Networks Intrusion Prevention System (IPS) to recognize a specific event and provide notification to ASM. It also provides steps for creating an ASM rule that responds to the events sent from Extreme Networks IPS.

Before you begin:

- Populate the Console database. Refer to the Console Help to Discover, Import, or manually Add network elements that you want to protect with ASM.

  TIP: Spend some time creating Device Groups that are meaningful for your network. Although Console provides pre-defined folders, you'll find that creating your own *unique* device groups makes it easier to define ASM Search Scopes later. For example, create new groups for your network elements organized by geographic region, data center, building, floor, etc., then drag and drop devices into these new groups.

- Define an SNMPv3 Credential with AuthPriv access. Refer to the Authorization/Device Access help topic for more information.
- You should know:
  - The IP Address or hostname of the system on which you are running Extreme Networks IPS .
  - The username and password with administrator access to Extreme Networks IPS.
  - The IP Address or hostname of the system on which you are running ASM.

The Getting Started exercise consists of the following tasks:

- Configure NetSight's SNMPTrap Service - Configure user credentials used with SNMPv3 trap messages.

- Configure the Extreme Networks IPS - Create a simple event trigger and configure notification to ASM.

- Configure Automated Security Manager - Create a rule to recognize a trap from the Extreme Networks IPS host device and record an event in the ASM

Activity log.

- Trigger a Test Trap - Trigger a trap by attempting to access the Extreme Networks IPS host using the community name *PRIVATE* and verify an event is recorded in the ASM Activity log.

Configure the SNMP Trap Service

Extreme Networks IPS uses *Inform* messages to notify ASM of a threat, which means that the NetSight SNMPTrap Service (snmptrapd) must know the user credentials of the sending agent (on the Extreme Networks IPS device) before the SNMPTrap Service can receive the message. If this information is not provided, the SNMPTrap Service drops the trap messages. To learn more about Traps and Informs, read the Traps and Informs help topic. The user credentials configured here must match the user credentials configured on Extreme Networks IPS.

You can configure SNMPTrap information by adding user information to the snmptrapd.conf file using a text editor.

1. Launch NetSight ASM.
2. From the **Tools** menu, select **Modify snmptrapd.conf**.
3. The `snmptrapd.conf` file opens.
4. Add an SNMPv3 user credential using the following format:

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

Where:	
myUser	security user name.
myauthpassword	`MD5` or `SHA` - authentication type and authentication password (optional parameter - do not use when authentication is not used).
myprivpassword	`DES` - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

5. Save the snmptrapd.conf file before closing.

6. Any time the snmptrapd.conf file is changed, the SNMPTrap Server must be restarted.

Windows	**Linux**
a. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar). b. Right-click the Services Manager icon (▣). c. Select **SNMP Trap** > **Restart**.	a. Navigate to the `etc/init.d` directory. b. Type the command: `nssnmptrapd stop` c. Press **Enter**. d. Type the command: `nssnmptrapd start` e. Press **Enter**.

Configuring the Intrusion Prevention System

In its simplest form, IPS configuration consists of triggering events related to specific threats, constructing messages sent to ASM whenever one of these threats is detected, and then configuring the notification to ASM.

For this exercise, we are setting up an event to test the connection from the IPS to ASM. The following steps create a very simple event trigger (access the Extreme Networks IPS host with the Community Name *PRIVATE*), then configure notification to ASM using the SNMPv3 Credential added earlier to snmptrapd.conf file.

The following steps provide examples and instructions for configuring Extreme Networks IPS with this test message. (If you are using a different IPS, refer to that product's documentation to configure the corresponding features.) You must have an EMS management client application installed on your machine to perform these steps. (Refer to the *Extreme Networks IPS Installation Guide* for installation instructions.)

1. Open the EMS management client application using the normal start method for your operating system. For example, on Windows, click Start > EMS Client > EMSClientWindow. A login window appears.
2. Enter your username and password.

3. Click on the **Alarm Tool Policy View** icon. The Alarm Tool lets you create Event Groups that describe specific network threats and how the system responds when those threats are detected.
4. Expand the **Custom Policies** folder to view the custom policies.
5. Click on any existing custom policy.
6. Click on the right-panel Event Groups tab.
7. Create a new Event Group.
    a. Click **New** to open the Event Group Editor.
    b. In the left column, expand the Vulnerability category and select SNMP:PRIVATE. Click on **Add** to move it to Event Group in the right column.
    c. Enter an Event Group Name and click **OK**.
    d. Click on **Commit**. The new Event Group is displayed in the table under Event Group.
8. Click the right-panel Notification Rules tab.
9. Create a new Notification Rule.
    a. Click **New** in the left pane of the window. Give the notification a name, specify a Time Period of None, and click **OK**. The new notification rule is listed under Notification Rules.
    b. Click on the new notification rule to highlight it.
    c. Click on the NetSight ASM sub-tab in the right pane. (If the NetSight ASM tab is not visible, use the arrows to locate it.)
    d. Click **New** in the right pane to open the NetSight ASM Editor.
    e. Enter or select the following:
        - Server - Enter the ASM host IP address. (Do not use the IP address of a NetSight ASM client-only PC.)
        - Security Name - Enter the SNMPv3 Credential - User Name you configured in the snmptrapd.conf file.
        - Auth Password - Enter the SNMPv3 Credential - Auth Password you configured in the snmptrapd.conf file.
        - Priv Password - Enter the SNMPv3 Credential - Priv Password you configured in the snmptrapd.conf file.
        - ASM Category - Select ASM_ATTACKS.

   f. Click **OK**.

10. Click the right-panel Global Options tab and then select the SNMP sub-tab.
11. Enter the IP address of the EMS server sending the SNMP traps.
12. Click on the right-panel Alarms tab.
13. Create a new Alarm.
    a. Click **New** to open the Alarm Editor.
    b. Enter a **Name** for your new Alarm.
    c. Select **Real Time** from the drop-down menu in the **Type** field.
    d. Leave the **Summary Interval** set to its default value (3600 milliseconds).
    e. Select the name of your new *Event Group* from the drop-down menu in the **Event Group** field.
    f. Leave **Filter** set to None.
    g. Leave **Threshold** set to None.
    h. Select the name of your new *Notification Rule* from the list in the **Notification Rules** field.
    i. Click **OK**.
14. Click on **Commit**.
15. Deploy your new trap configuration.
    a. Click on the **Enterprise View** icon.
    b. Right-click on the Alarm Tool: *notification name* that you created and select **Associate Alarm Tool Policy**.
    c. Select the new policy and click **OK**.
    d. Right-click on the Alarm Tool: *notification name* that you created again and select **Deploy** from the drop-down menu.

Configuring Automated Security Manager

The following steps create an action rule to recognize any trap from the Extreme Networks IPS host device and record the event in the ASM Activity Log.

1. In ASM, select **Tools > ASM Configuration** from the menu bar.
2. Click on the **Edit** radio button, located in the top left section of the window.

3. In the Groups and Devices tree, select My Network and click **Include**. Click **Continue**.
4. Click **Continue** in the **Excluded Port Types** view.
5. Click **Continue** in the **Exclude Specific Ports** view.
6. Click **Create** in the **Rule Definitions** view. The Create Rule window opens.
7. Enter a **Name** for the new rule and click **Apply**, then **Close**.
8. Leave the remaining settings set to their default values. This allows matching any event category, recording the event in the ASM Activity Monitor, but no action will be taken.
9. Click **Save** and then **Close** in the ASM Configuration window.
10. Leave the ASM Activity Monitor window open so you can view the log while triggering a test trap message.

Trigger a Test Trap

To test the connection between Extreme Networks IPS and ASM, we will use MIB Tools to attempt to access the Extreme Networks IPS host using the community name *PRIVATE*.

1. In the ASM Activity Monitor window, make sure that the Operation Mode is set to either **Search and Respond** or **Search Only**.
2. In the Console main window, right-click on the Extreme Networks IPS device in the left-panel tree and select MIB Tools from the menu.
3. Select **Use SNMPv1** from the Select Protocol drop-down menu in the upper right of the MIB Tools window and enter *PRIVATE* as the Community Name. Click **Contact**.

You now see one or more traps recorded in the ASM Activity Monitor. If this does not occur, review the preceding steps, checking for errors.

What's Next

If you successfully triggered and recorded a trap in ASM, you're ready to configure additional Extreme Networks IPS events and enable ASM to provide responses to protect the integrity of your network.

In the preceding exercise we triggered a trap message to ASM for a specific event (logging on using the community name, PRIVATE). ASM recognized the trap because it matched the character string defined by the ***Enterasys Networks'***

Threat Notification MIB object, `etsysThreatNotificationThreatCategory`, in this case ASM_ATTACKS, with a corresponding Event Category defined in ASM. To be recognized by ASM, the text string in the event messages sent by an IPS must match exactly with an Event Category name defined in ASM. (Event categories are defined in ASM Configuration - Rule Variables.)

Extreme Networks IPS has four default notification rules: netsight-atlas-asm-attacks, netsight-atlas-asm-compromise, netsight-atlas-asm-informational, and netsight-atlas-asm-misuse. Each of the Extreme Networks IPS default notification rules has a corresponding default event category in ASM: ASM_ATTACKS, ASM_COMPROMISE, ASM_INFORMATIONAL, and ASM_MISUSE. ASM uses Rules to compare incoming trap messages with specific event categories, then determines where and what action to apply as a response.

For ASM's response to a serious threat to be timely and effective, it is important that ASM only be notified of serious threats. The following table lists the Extreme Networks IPS events for which notification to ASM is recommended:

BACKDOOR:PHATBOT	COMP:MS-DIR	COMP:ROOT-ICMP
COMP:ROOT-TCP	COMP:ROOT-UDP	COMP:SDBOT-LOGIN
COMP:SDBOT-NETINFO	COMP:SPYBOT-DOWNLOAD	COMP:SPYBOT-INFO
COMP:SPYBOT-KEYLOG	COMP:WIN-2000	COMP:WIN-XP
GENERIC:UPX-EXE	MS-BACKDOOR	MS-BACKDOOR2
MS-BACKDOOR3	MS-SQL:HAXOR-TABLE	MS-SQL:PWDUMP
MS-SQL:WORM-SAPPHIRE	MS:BACKDOOR-BADCMD	MS:BACKDOOR-DIR
SMB:SAMBAL-SUCCESS	SSH:HIGHPORT	SSH:X2-CHRIS
SSH:X2-CHRIS-REPLY		

Read the ***Extreme Networks IPS Configuration Guide*** (accessed from the EMS client Help menu) to learn more about events, alarms, traps, and inform configuration in Extreme Networks IPS.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Create/Edit Rule Window
- Incident Test Tool

For information on related tasks:

- How to Set ASM Options
- How to Create/Edit Rule Window
- Using the Incident Test Tool

How to Use Automated Security Manager

The How To section contains Help topics that give you instructions for performing tasks in Extreme Management Center Automated Security Manager.

How to Configure the SNMP Trap Service

Console's SNMPTrap Service (snmptrapd) must know the user credentials of a sending agent (on the device) before receiving a trap. If this information is not provided, the SNMPTrap Service drops trap messages.

There are two ways to configure Trap Receiver information: Using the Console's Trap Receiver Configuration window or by manually adding user information to the snmptrapd.conf file using a text editor. Instructions for the latter are provided in the `snmptrapd.conf` file, located on the server in the `<install directory>\NetSight\appdata` directory.

Using the Trap Receiver Configuration Window

The Trap Receiver Configuration view is accessible from the right-click menu when clicking a device in Console's left (tree) panel.

NOTES:

1. Changes you make in this window alter the `snmptrapd.conf` file. The `snmptrapd.conf` file is located on the server in the `<install directory>\NetSight\appdata` directory. After making changes, you must restart the SNMPTrap Service on the NetSight Server. Refer to Restarting snmptrapd for more information.
2. The `snmptrapd.conf` is not preserved during the Console Uninstall.

1. In Console, expand the left panel, right-click on one or more devices or device groups, and select Trap Receiver Configuration.
2. Click the **snmptrapd** tab.
3. Click Add Entry. This adds a new row to the table.
   For the next step, you'll need an SNMPv3 Credential. If you do not already have a credential defined, go to the Authorization/Device Access - Profiles/Credentials tab, where you can create one. Otherwise, proceed to Step 4.
4. Click in the **Credential Name** column for the device on which you want to set a specific SNMPv3 credential and select your SNMPv3 AuthPriv credential from the drop-down menu. The **snmptrapd.conf Text** area shows the text of your entry in the configuration file.

You can also type user credentials directly into the snmptrapd.conf Text area to add entries to the configuration file. The format for user information is:

```
createUser username (MD5|SHA) passphrase [DES passphrase]
```

Example - for an AuthPriv user, enter the following line in the file:

```
 createUser myAuthPrivUser MD5 mypassword DES
myotherpassword
```

Where *myAuthPrivUser* is the security user name, *mypassword* is your authentication password and *myotherpassword* is your encryption password. The authentication and privacy parameters are optional, depending on whether you are using authentication and/or privacy.

5. Click **Save** and **Close**. The user credentials are added to the snmptrapd.conf file.

Restarting snmptrapd Service

Depending on the system where the NetSight Server is running and your preference, there are several ways to restart the snmptrapd service.

Restarting the service locally on the NetSight Server host system:

Windows	Linux
Using the Services Manager: a. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar). b. Right-click the Services Manager icon ( ). c. Select **SNMPTrap** > **Restart**. Using Windows Services: a. From the Control Panel, access the Administrative Tools > Services window. b. Locate the snmptrapd service and select "Restart the service."	a. Navigate to the `etc/init.d` directory. b. Type the command: `nssnmptrapd stop` c. Press **Enter**. d. Type the command: `nssnmptrapd start` e. Press **Enter**.

Restarting the service remotely from a NetSight Client host system:

Windows	**Linux**
Restarting the service remotely on Windows host systems is only possible if both the Client and Server are capable of running **Remote Desktop** (a feature of Windows XP Professional) or through the use of a third-party facility that provides similar capabilities to Remote Desktop. When you can access the Services Manager on the remote system using either Remote Desktop or a third-party program, you can restart the service as follows: a. Go to the Taskbar Notification Area of the remote desktop. b. Right-click the Services Manager icon (E). c. Select **SNMPTrap** > **Restart**.	a. Telnet to the server and login as an administrative user. b. Navigate to the `etc/init.d` directory. c. Type the command: `nssnmptrapd stop` d. Press **Enter**. e. Type the command: `nssnmptrapd start` f. Press **Enter**. g. Log out and close the telnet session.

Related Information

- Traps and Informs

How to Create and Edit ASM Rules

Automated Security Manager rules serve two distinct functions:

1. Examine the source of the threat (switch/port) to determine if certain conditions exist (e.g. threat category, source of the notifying IPS, policies currently applied to the port, etc.) that warrant a response.
2. Define the action to be taken when these conditions match the criteria defined by the rule.

The Create Rule and Edit Rule windows are identical. They are accessed from the Automated Security Manager Configuration Window's Rule Definitions view. The only difference between the two windows is that the Edit Rule window contains the definition for a particular rule selected in the Rule Definitions view.

Information on:

- Editing a Rule
- Creating a Rule

Editing a Rule

To edit an existing rule:

1. Select a rule from the table in the Automated Security Manager Configuration Window's Rule Definitions view.
2. Click **Edit**. The **Edit Rule** window opens.
3. Go on to Step 2 in the Creating a Rule section to modify the parameters for the rule as necessary.

Creating a Rule

To create a new rule:

1. Click **Create** in the ASM Configuration Window's Rule Definitions view. The Create Rule window opens.
2. Type a **Name** for the rule. The name can be any character string, excluding spaces, up to 64 characters.

3. Define the **Conditions To Test For** that ASM uses to determine if and how to respond to a particular event:
   a. Expand the device tree in the **Group & Devices** panel to select a target device or device group eligible for the action specified in the rule. For example, do not select a device/device group for a device type that does not support policy if you are creating a rule with an action that applies a policy. Or as another example, in some rules, you may want to apply different actions or more or less permanent actions for certain subnets containing critical network resources. You can create several rules that address a particular threat and apply different actions based on your target.
   b. Select the Event Categories that result in applying the action for this rule. To be recognized by ASM, the text string in the event message sent by the IPS must exactly match the event category names in the rule.
      - **Match Any** - This is an unconditional match for the category.
      - **Match Selected** - The event category is compared against one or more categories selected from the list.
      - **Exclude Selected** - The event category matches if it is not one of the categories selected from the list.

   Extreme Networks IPS has four default notification rules: netsight-asm-attacks, netsight-asm-compromise, netsight-asm-informational, and netsight-asm-misuse. Each notification rule has a corresponding event category in ASM: ASM_ATTACKS, ASM_COMPROMISE, ASM_MISUSE, and ASM_INFORMATIONAL.

   For ASM's response to a serious threat to be timely and effective, it is important that ASM only be notified of serious threats. The following table lists the Extreme Networks IPS events for which notification to ASM is recommended:

BACKDOOR:PHATBOT	COMP:MS-DIR	COMP:ROOT-ICMP
COMP:ROOT-TCP	COMP:ROOT-UDP	COMP:SDBOT-LOGIN
COMP:SDBOT-NETINFO	COMP:SPYBOT-DOWNLOAD	COMP:SPYBOT-INFO
COMP:SPYBOT-KEYLOG	COMP:WIN-2000	COMP:WIN-XP
GENERIC:UPX-EXE	MS-BACKDOOR	MS-BACKDOOR2
MS-BACKDOOR3	MS-SQL:HAXOR-TABLE	MS-SQL:PWDUMP
MS-SQL:WORM-SAPPHIRE	MS:BACKDOOR-BADCMD	MS:BACKDOOR-DIR

SMB:SAMBAL-SUCCESS	SSH:HIGHPORT	SSH:X2-CHRIS
SSH:X2-CHRIS-REPLY		

c. Select the Sender Identifiers that result in applying the action for this rule. This is a unique identifier associated with the intrusion prevention system that detected the security event.

   - **Match Any** - This is an unconditional match for the Sender ID.
   - **Match Selected** - The Sender ID is compared against one or more Sender Identifiers selected from the list.
   - **Exclude Selected** - The Sender ID matches if it is not one of the Sender Identifiers selected from the list.

d. Select the Policies that result in applying the action for this rule. This attribute examines policies currently applied on the port.

   - **Match Any** - This is an unconditional match for a currently applied policy.
   - **Match Selected** - The currently applied policy is compared against one or more policies selected from the list.
   - **Exclude Selected** - The currently applied policy is not one of the policies selected from the list.

e. Select the VLANs that result in applying the action for this rule. This attribute examines VLANs currently applied on the port.

   - **Match Any** - This is an unconditional match for a currently applied VLAN.
   - **Match Selected** - The currently applied VLAN is compared against one or more VLANs selected from the list.
   - **Exclude Selected** - The currently applied VLAN is not one of the VLANs selected from the list.

f. Select the Day and Time Ranges that result in applying the action for this rule.

4. Define the action taken when the event matches the above rule criteria. You can define one of three Standard ASM Actions, define a Custom Action, or define both a Standard Action and a Custom Action. When both are defined, ASM attempts to apply both actions. If either one fails, then the other action may still be applied.

NOTES:

1. Take care when defining both a standard and custom action for a rule. Ensure the two actions are independent. For example, create a standard action that applies a PVID on a port with a custom action that runs a script. The script assumes the PVID is applied and works to find the port on which the apply PVID failed.
2. With one exception, you can undo applied actions. The exception occurs when two actions are defined within a rule: a standard ASM action and a custom action. If the standard ASM action fails, the custom action is applied and, if successful, cannot be undone. Under these circumstances, configure your custom action to take into account the potential failure of the standard ASM action.

a. Standard ASM Actions: Select one of four standard ASM actions.

- None - Take no action for this event.
- Disable Port - Disable the port that is the source of the threat. The port can be disabled permanently or for a specific interval, depending on the Duration setting.
- Apply Policy - A Policy you select can be applied to the port, either permanently or for a specific interval, depending on the Duration setting.

  When Apply Policy is selected and the threat is located on a port on a device that supports Multi-User Authentication (e.g., N-Series), you can apply a policy to a specific MAC address or IP address. This lets you isolate a single user instead of affecting all users on the port. You can apply a user-specific policy to an IP address or MAC address instead of changing the port policy. If the threat MAC Address is unique to a particular Threat IP (typically on devices at the edge of your network), select MAC to apply the policy to the MAC address and override its port or dynamic policy. If the threat is on a device at the core of your network and the MAC Address maps to several IP Addresses, select IP to apply the policy to the IP Address and override its port or dynamic policy.

  NOTE: Policies applied to a MAC source override policies applied to an IP source. So, if there is a policy currently applied to a MAC source, applying a policy to an IP source has no effect.

- **Apply PVID -** You can select a PVID from the associated drop-down menu and apply it to the port. The PVID Egress drop-down menu lets you either retain the current PVID egress state by selecting **None** or change the egress state to **Untagged**. When **Untagged** is selected, the PVID is applied and the egress state is set to **Untagged**. When **None** is selected, the egress state is unchanged and only the PVID is applied. If you have specified a Discard VLAN as the PVID, selecting **None** typically indicates traffic is discarded.
- **Notify NAC -** When you select Notify NAC, ASM notifies NAC Manager in response to a real-time security threat from an end-system on the network. NAC Manager automatically adds the end-system's MAC address to the Blacklist end-system group, effectively putting the end-system in quarantine and preventing the end-system from accessing the network from any location.

b. **Custom Action:** Check **Custom Action** and click **Edit** to open the Specify Program for Action window, where you can customize the response to an event by selecting a program to be executed.

   i. In the **Program to run** field, type a script name, if known or use the **Select** button to open a file browser window and choose a script. The **Program to run** field does not allow using options. For example, you cannot enter `myscript.bat –i <IP Address> -m <MAC Address>` in the **Program to run** field.

TIP: To execute a script with options, create a script without options that executes another script that has options (Windows only). For example:

1. Create a script named, `asm_script.bat` with an entry to call `myscript.bat` such as: C:\Program Files\My Custom Files\myscript.bat –i %1 -m %2".
2. Uncheck all but the **Threat IP** and **Threat MAC** checkboxes and select **Unformatted without spaces** (don't send any keyword (thip= or thmac=) to your script.). The variable %1 returns <*Threat IP Address*> and %2 returns the <*Threat MAC Address*>.

   If you are using PERL script, use a different argument variable, such as $ARGV[0] (First argument) or @ARGV (all arguments). Using the shell script is similar to a Windows batch file script (%1 for the first argument, %* for the all arguments).

ii. Select elements of the threat message to pass to your program from the Parameters to pass to program area.

iii. Select the format used for the information passed to your program.

- When Formatted with keyword is selected, your program passes the parameters using a format that includes a keyword associated with each parameter (e.g., **`keyword="value"`**). So, for example, if Sender Name is selected as a parameter, the keyword sname is used and the information passed to the script would be **`sname="dragon_id"`** followed by a space and then the keyword and value for the next parameter. The following table defines the keywords for each parameter and the order that the values are passed to the script (listed from top to bottom in the table).

Parameter	Keyword
Sender Name	sname
Sender ID	sid
Event Category	ecat

Parameter	Keyword
Signature	sig
Incident Number	incident
Threat IP	thip
Threat MAC	thmac
Device IP	dev
Device Port	port
Rule Name	rname
Action	action
Details	dtls
SNMP Parameters	see Note 1
Status	stat

Note 1: When you select an SNMP parameter, the **snmp=**_value_ indicates the SNMP version and the subsequent parameters contain the values assigned for the credentials associated with the device. When you select multiple SNMP parameters (e.g., SNMP Write and SNMP Read) the script uses the values for the highest access level.

SNMP v1, SNMPv2		SNMPv3	
Parameter	**Keyword**	**Parameter**	**Keyword**
SNMP Read	snmp="v1" ro	SNMP Read, SNMP Write, SNMP SU/Max Access	snmp="v3" user seclevel authtype authpwd privtype privpwd
SNMP Read	snmp="v1" rw		
SNMP Read	snmp="v1" su		

Example:

If Sender Name, Sender ID, Threat MAC, and SNMP Write are selected and the device is configured for SNMPv1 credentials, the information passed to the script appears as:

```
sname="my sender name" sid="dragon id"
thmac="00.00.1d.11.22.33" snmp="v1"
rw="public"
```

And, for a script named **myscript.bat**, the resulting script command is executed as:

```
C:\Program Files\Extreme
Networks\NetSight\appdata\AutoSecMgr\scripts\m
y_script.bat sname="my sender name"
sid="dragon id" thmac="00.00.1d.11.22.33"
snmp="v1" rw="public"
```

- When **Unformatted without spaces** is selected, the parameters are passed as space delimited, unformatted text, without keywords. For this option, your script must know which parameters are being passed the order in which they are passed. If a parameter contains any spaces, the script replaces them with an underscore (_).

  Example:

  You select Sender Name, Sender ID, Threat MAC, and SNMP Write and the device is configured for SNMPv1 credentials, the information passed to the script appears as:

  ```
  my_sender_name dragon_id 00.00.1d.11.22.33 v1
  public
  ```

  And, for a script named **myscript.bat**, the resulting script command is executed as:

  ```
  C:\Program Files\Extreme
  Networks\NetSight\appdata\AutoSecMgr\scripts\m
  y_script.bat my_sender_name dragon_id
  00.00.1d.11.22.33 v1 public
  ```

iv. Click **OK**.

c. You can specify a notification to be part of the rule's action. For example, you can specify an E-Mail notification sent in response to a threat. Check **Notification** and select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window, which lists the configured notifications. In this window, you can select a Notification to edit, or click **Create** to open the Create Notification window.

   d. Click **Manual Confirmation Required** if the action requires manual confirmation before being applied.

5. Specify an action to undo.
   a. Define the **Time before Undo** for the selected action as **Permanent** or set to a time span of **Minutes**, **Hours, Days**, as defined in the associated field. **Permanent** means that ASM does not automatically undo the action after a certain time interval, but it can still be manually undone.
   b. Check **Custom Undo** and click **Edit** if you want to specify an action taken when an action is undone. This opens the Specify Program for Undo window.
      i. In the **Program to run** field, type a script name if known, or use the **Select** button to open a file browser window and choose a script. The **Program to run** field does not allow using options. For example, you cannot enter `myscript.bat -i <IP Address> -m <MAC Address>` in the Program to run field. See the Tip above for more information.

         NOTE: When a custom undo action script does not specify the path for its output, the output is placed in the `<install directory>\NetSight\jboss\bin directory.`

      ii. Select elements of the threat message to pass to your program from the **Parameters to pass to program** area.
      iii. Select the format used for the information passed to your program.
      iv. Click **OK**.
   c. You can specify a notification to be part of the rule's undo action. Check **Notification** and select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window, which lists the configured notifications. In this window, you can select a Notification to edit, or click **Create** to open the Create Notification window.

When you are satisfied with the settings for your rule, click **Apply** and then **Close**. Your rule appears *Enabled* in the Rule Definitions view table.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Activity Monitor

For information on related tasks:

- Using the ASM Activity Monitor

How to Send a Test Incident to ASM

This tool lets you test and debug the search scopes, and actions to verify ASM's response to an event. You can perform a basic test that sends a inform message directly to ASM, bypassing the SNMPTrap Service or you can configure a more comprehensive test to test the complete path (IDS to SNMPTrap Service/Console to ASM), simulating exactly the workings of an actual inform message. This more comprehensive test requires that the SNMP message be correctly specified (including authentication credentials) and that Console's SNMPTrap Service is running.

NOTES:

1. Your client system must have SNMP access to the server to use the **Test response by sending an SNMP trap to ASM** level of testing.
2. The NetSight SNMPTrap Service (snmptrapd) must be configured with Security User credentials and/or Engine IDs for devices from which Console's SNMPTrap Service (snmptrapd) accepts SNMPv3 Notification messages. Without this information, the SNMPTrap Service drops notification messages. The traps do not appear in the Events view and ASM does not receive notification. Refer to How to Configure the SNMPTrap Service to learn more about configuring SNMPTrap Service.

To test a response by sending threat information directly to ASM:

1. Select Test a response by sending threat information directly to ASM.
2. Set the parameters under the heading Specify parameters of test incident for the test incident that will be sent to ASM:
   - Sender ID - This is a unique identifier associated with the intrusion detection system that detected the security event.
   - Sender Name - The sender name being tested. This is a unique name associated with the intrusion detection system that detected the event. Sender Names are case sensitive.
   - Threat Category - The event category being tested. ASM's default event categories categories are ASM_ATTACK, ASM_COMPROMISE, ASM_INFORMATIONAL, and ASM_MISUSE. Event Category Names are case sensitive.
   - Signature - A signature provides a unique identifier for the threat being tested.

- **Threat IP** - The address where the threat is detected and where ASM applies an action if one is configured for this threat.

3. Click **Send Incident to ASM**. Your incident appears in the table in the ASM Monitor window.

To perform a more comprehensive test:

1. Select **Test response by sending an SNMP trap to ASM**.
2. Set the parameters for the basic test (**Specify parameters of test incident to be sent to ASM**).
3. Set the parameters under the heading **Specify additional parameters for sending SNMP trap**.
    - **SNMPv3 User Name** - The user name of the simulated user.
    - **Authentication Type** - The authentication method used for the inform (MD5 or SHA) message.
    - **Authentication Password** - The authentication password of the simulated user.
    - **Privacy Type** - The encryption method used for the inform (DES or None) message.
    - **Privacy Password** - The encryption password for the simulated user.
    - **Trap Receiver** - The system on which the SNMPTrap Service is running.
4. If necessary, edit the SNMPTrapd.conf file to configure user credentials in Console's SNMPTrap Service. (Refer to How to Configure the SNMPTrap Service for more information about editing this file.)
5. Click **Send Incident to ASM**. Your incident appears in the table in the ASM Monitor window.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Automated Security Manager Activity Monitor

For information on related tasks:

- How to Set Automated Security Manager Options
- How to Create and Edit Automated Security Manager Rules
- How to Use Automated Security Manager Activity Monitor

How to Set ASM Options

Automated Security Manager Options (**Tools > Options**) let you define your preferences for ASM operations. The right-panel view changes depending on what you select in the left-panel tree. Expand the Automated Security Manager folder to view all the different options you can set.

Instructions on setting the following ASM options:

- Advanced Settings
- Action Limits
- Dialog Boxes
- SNMP

Advanced Settings

If you have created a rule with an action that requires a manual confirmation before the action is taken and an email notification has been configured for the action, the Advanced Settings view option causes ASM to also send an email notification when the action needs to be confirmed. The subject line of the notification is "Awaiting Manual Confirmation." Once the action has been performed, the notification is sent again with the subject line originally defined in the notification. (Rule actions and notifications are configured in the Create Rule window.)

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Click **Advanced Settings** in the left panel of the ASM Options window.
3. Select the checkbox to send a notification when an action is awaiting confirmation.
4. Click **Apply** or **OK**.

Setting Action Limits

The Action Limits view lets you set limits for Automated Security Manager's threat responses.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Click **Action Limits** in the left panel of the ASM Options window.

3. Set the **Max Number of Outstanding Actions** to limit the number of outstanding (pending execution) actions.
4. Set the **Max Number of Actions per Threat** to limit on the number of actions executed for a given threat. Both pending and executed actions count toward the maximum. When the limit is reached, no further actions are executed for the threat.
5. Click **Apply** or **OK**.

Dialog Boxes

The Dialog Boxes view lets you select whether certain dialog boxes are shown or ignored.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select **Dialog Boxes** in the left panel of the ASM Options window.
3. Select or deselect the checkbox depending on whether you want the Edit Mode Required dialog box displayed or ignored. This dialog appears if you try to make changes in the ASM Configuration window without first selecting Edit Mode. Deselecting the checkbox means that the dialog does not appear and you are automatically changed to Edit Mode.
4. Click **Apply** or **OK**.

Related Information

For information on related windows:

- Automated Security Manager Activity Monitor
- Automated Security Manager Configuration Window
- Automated Security Manager - Create/Edit Rule Window

For information on related tasks:

- How to Use the Automated Security Manager Activity Monitor
- How to Create and Edit Automated Security Manager Rules

How to Use the ASM Activity Monitor

The Activity Monitor opens when you launch Automated Security Manager (ASM). It contains a log of ASM activities, and provides access to features that let you manage responses to network security threats.

Information on:

- Set ASM's Operation Mode
- Confirm Responses
- Undo Selected Actions
- Delete Table Entries
- Clean Up Incidents

Setting ASM's Operation Mode

ASM can be fully enabled, completely disabled, or set to only search for and record network threats:

- Click **Disabled** to set ASM to an inactive state. In this condition, ASM ignores events from the intrusion detection system and neither seeks out nor responds to the sources of network threats.
- Click **Search Only** to set ASM to recognize security threats, identify their source ports, and record event information in the Activity Monitor, but not to respond.
- Click **Search and Respond** to enable all of ASM's features. In this state, ASM is fully active; threats are recognized, sources identified, and responses (actions) are applied.

Confirming Actions for Selected Log Entries

Actions configured for **Manual Confirmation Required** allow you to examine specific events before taking an action:

1. Select one or more events from the Activity Monitor.
2. Click **Confirm Response** to apply the configured actions.

Undo Action

You can reverse the most recent actions on selected event/action entries in the Activity Monitor:

1. Select one or more events from the Activity Monitor.
2. Click **Undo Selected Actions**.

Delete Table Entries

You can remove selected event/action entries from the Activity Monitor:

1. Select one or more events from the Activity Monitor.
2. Click **Delete Table Entry**. The entries are removed without further confirmation.

Clean Up Incidents

You can delete incidents from the Activity Monitor based on incident status.

1. Click the **Clean Up Incidents** button below the Activity Monitor table. The Clean Up Incidents window opens.
2. Use the checkboxes to select the statuses of the incidents you want to delete. For more information on each status, see the Icon/Status section of the Activity Monitor Help topic.
3. Click **Apply**.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Create/Edit Rule Window

For information on related tasks:

- How to Set Automated Security Manager Options
- How to Create and Edit Automated Security Manager Rules

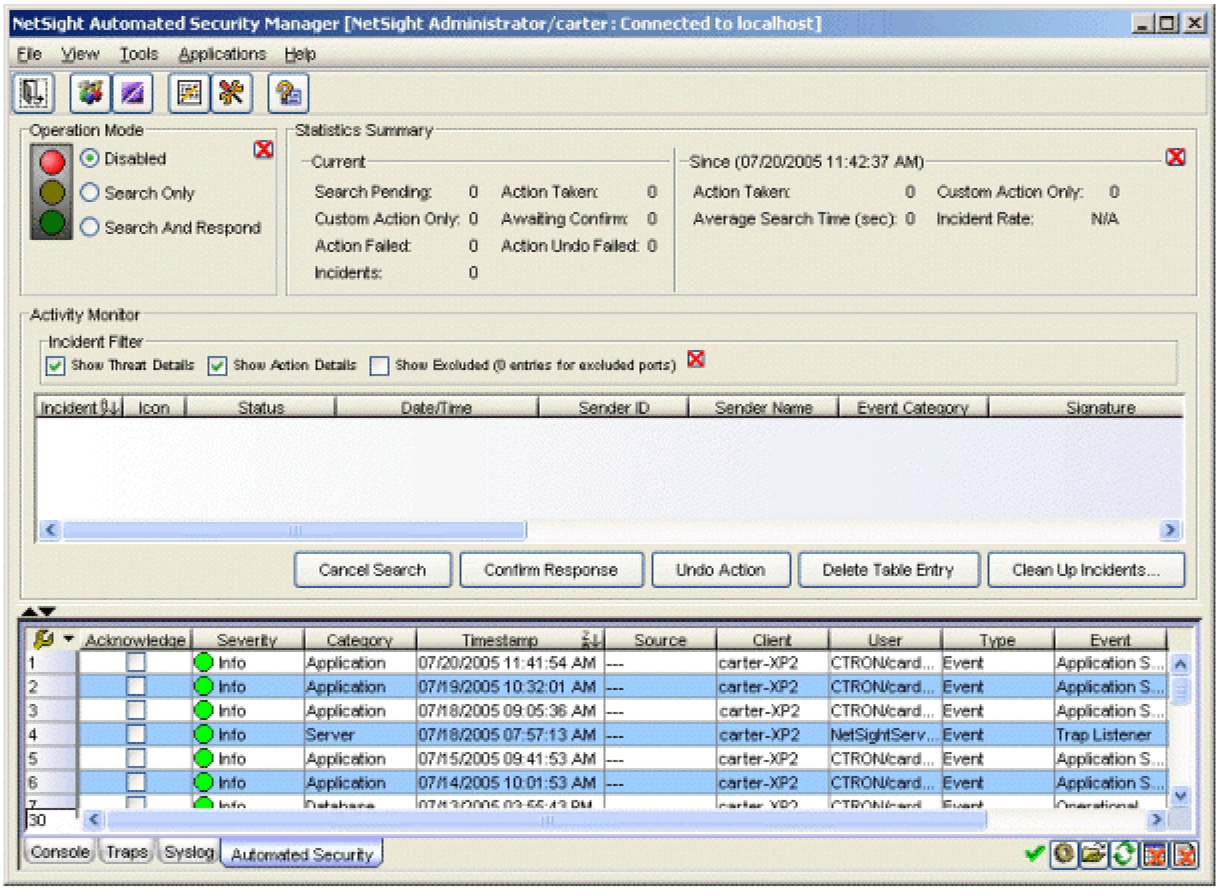
Automated Security Manager Windows

The Windows section contains Help topics describing Extreme Management Center Automated Security Manager windows and their field definitions.

ASM Activity Monitor

The Automated Security Manager Activity Monitor window consists of three major functional areas. The top section provides the ability to set ASM's operational mode and view statistics. The center section provides a log of ASM activities. The bottom section contains an Events View where you can view alarm, event, and trap information for ASM, Console, network devices, and other NetSight applications.

CAUTION: Do not attempt to manually remove actions applied to devices from NetSight Automated Security Manager. Use the **Undo Action** button in ASM's Activity Monitor window to undo a threat response. Attempting to manually remove actions can leave devices in an unspecified condition, possibly compromising the security of your network.



Operation Mode: ● Disabled ○ Search Only ○ Search And Respond

Current

Search Pending:	0	Action Taken:	0
Custom Action Only:	0	Awaiting Confirm:	0
Action Failed:	0	Action Undo Failed:	0
Incidents:	0		

Since (07/20/2005 11:42:37 AM)

Action Taken:	0	Custom Action Only:	0
Average Search Time (sec):	0	Incident Rate:	N/A

☑ Show Threat Details ☑ Show Action Details □ Show Excluded (0 entries for excluded ports)

	Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event
1	□	● Info	Application	07/20/2005 11:41:54 AM	---	carter-XP2	CTRON/card...	Event	Application S...
2	□	● Info	Application	07/19/2005 10:32:01 AM	---	carter-XP2	CTRON/card...	Event	Application S...
3	□	● Info	Application	07/18/2005 09:05:36 AM	---	carter-XP2	CTRON/card...	Event	Application S...
4	□	● Info	Server	07/18/2005 07:57:13 AM	---	carter-XP2	NetSightServ...	Event	Trap Listener
5	□	● Info	Application	07/15/2005 09:41:53 AM	---	carter-XP2	CTRON/card...	Event	Application S...
6	□	● Info	Application	07/14/2005 10:01:53 AM	---	carter-XP2	CTRON/card...	Event	Application S...
7	□	● Info	Database	07/13/2005 03:55:43 PM		carter-XP2	CTRON/card...	Event	Operational

30

The Operation Mode and Statistics Summary panels, as well as the Incident Filter, can be closed by clicking the ☒ button and restored from the View menu.

In addition, the Operation Mode panel can be restored from the Operation Mode Indicator's drop-down menu in the upper-right corner of the window. You can also restore the Incident Filter from a right-click menu selection in the Activity Monitor Table.

Operation Mode

You can display the full Operation Mode panel or iconize it in the main view (by clicking the ☒ button) to show only the *traffic light* indicator in the upper-right corner. You can select from the following options:

Disabled - When selected, Automated Security Manager is not active. It neither seeks out the sources of network threats nor responds to them.

Search Only - When selected, security threats are recognized, source ports are identified and the information is recorded in the Activity Monitor but, no response is applied.

Search and Respond - When selected, Automated Security Manager is fully active. In this state, threats are recognized, source ports are identified, and responses (actions) applied.

NOTE: The NetSight Server performs ASM searches using the profile for the server, not the profile for the ASM client user.

Statistics Summary

This area shows **Current** data and data accumulated **Since** the last statistics **Counter Reset**. The date/time stamp at the top of the area shows the time span during which the accumulated statistics are collected.

The **Tools > Statistics > Configure** menu option opens the ASM Statistics window, from which you can select the specific data elements displayed in the Statistics area. The **Tools > Statistics > Reset Counters** menu option resets the counters for the accumulated data and sets the timestamp to the current date and time. Refer to the ASM Statistics window for a description of specific data elements.

Activity Monitor

Incident Filter

This area lets you select the type of detailed information available in the table. Use the **Show Threat Details** or **Show Action Details** checkboxes to show or hide groups of columns in the Activity Monitor table. At least one detail selection (Show Threat Details, Show Action Details) must be active at any given time.

You can hide one or more columns in the table using the Table Tools > Settings or the Hide column from the right-click menu. However, reactivating either filter overrides the settings from the Table Tools or right-click menu and the columns associated with the filter are restored to the table.

- **Show Threat Details** - When checked, the table contains several columns that provide detailed threat information. Show Threat Details controls the **Date/Time**, **Sender ID**, **Sender Name**, **Event Category** and **Signature** columns.
- **Show Action Details** - When checked, the table contains several columns that provide detailed action information. Show Action Details controls the **Threat MAC**, **Device/Port**, **Rule Name**, **Action**, **Details**, **Last Update** and **Search Time** columns.
- **Show Excluded** - When checked, the table contains entries for IP addresses found on an excluded port.

Activity Table

Incident

This is an index of incidents in the Activity Monitor showing the order in which incidents were recorded. The sequence may be broken when incidents are removed from the table.

Icon/Status

The Icon and Status columns, taken together, indicate the status of a particular action response:

Icon	Status	Meaning
❗	Action Taken	Action successfully performed. • Port disabled • Policy replaced on port • Policy replaced for MAC • VLAN replaced for MAC • Port disabled and Custom Action Executed • Policy replaced on port and Custom Action Executed • Policy replaced for MAC and Custom Action Executed • VLAN replaced for MAC and Custom Action Executed • VLAN replaced on port and Custom Action Executed • Port disabled and Custom Action Failed • Policy replaced on port and Custom Action Failed • Policy replaced for MAC and Custom Action Failed
🕒	Timer in Progress	Undo Action waiting for timer expiration
❓	Action Awaiting Confirmation	• Action configured for Manual Confirmation and is not yet confirmed. • The status for this entry is *Action in Progress* when the ASM Operation Mode changed to *Disabled*, *Search Only* or Console is exited and relaunched.
⚠	Action Suspended (these entries are always eligible for Undo)	• Operation Mode changed to Search Only and the action is pending or timer in progress. • Operation Mode changed to Disabled (or Console exits and relaunches) and the entry is action pending or timer in progress.

Icon	Status	Meaning
⚠	No Action Can Be Taken	• No port found for threat IP address • Policy not supported on device (where action was Apply Policy) • No Rule matches the criteria for applying action • Port already disabled • Policy already applied to port • PVID already applied to port • Port already disabled, Custom action executed • Policy already applied to port, Custom action executed • PVID already applied to port, Custom action executed • Policy not supported on device, Custom action executed • Port already disabled, Custom action failed • Policy already applied to port, Custom action failed • PVID already applied to port, Custom action failed • Policy not supported on device, Custom action failed
⚠	Action Threshold Exceeded	• Too many ports for Threat IP address, action not taken • Too many actions in progress, action not taken • Too many ports for Threat IP address, action not taken, Custom action not executed • Too many actions in progress, action not taken, Custom action not executed

Icon	Status	Meaning
❌	Action Failed	• Device not reachable • SNMP Profile has *ReadOnly* access level • SNMP Sets fail (*Write* parameters do not match the device) • Device not in database • Policy not on device • Port cannot be disabled • Incomplete Trap information • VLAN ID not on device • VLAN Name not on device • Device not reachable, Custom action executed • SNMP Profile has ReadOnly access level, Custom action executed • SNMP Sets fail (*Write* parameters do not match the device), Custom action executed • Device not in database, Custom action executed • Policy not on device, Custom action executed • Port cannot be disabled, Custom action executed • VLAN ID not on device, Custom action executed • VLAN Name not on device, Custom action executed • Device not reachable, Custom action failed • SNMP Profile has *ReadOnly* access level, Custom action failed • SNMP Sets fail (*Write* parameters do not match the device), Custom action failed • Device not in database, Custom action

Icon	Status	Meaning
		failed - Policy not on device, Custom action failed - Port cannot be disabled, Custom action failed - VLAN ID not on device, Custom action failed - VLAN Name not on device, Custom action failed

Icon	Status	Meaning
✗	Action Undo Failed	• Current port state does not agree with ASM action taken • Current port policy setting does not agree with ASM action taken • Original policy does not exist on device • Current PVID setting does not agree with ASM action taken (this includes PVID and tagging parameters) • Current port state does not agree with ASM action taken, Custom action executed • Current port policy setting does not agree with ASM action taken, Custom action executed • Original policy does not exist on device, Custom action executed • Current PVID setting does not agree with ASM action taken, Custom action executed • Current PVID setting does not agree with ASM action taken; Custom action failed • Current port state does not agree with ASM action taken; Custom action failed • Current port policy setting does not agree with ASM action taken; Custom action failed • Original policy does not exist on device; Custom action failed • Current PVID setting does not agree with ASM action taken; Custom action failed

Icon	Status	Meaning
Blank	Action Taken and Undone	- Action undone by *Undo Action* button - Action undone by Timer - Action undone by *Undo Action* button; *Custom Undo Action* executed - Action undone by Timer; *Custom Undo Action* executed - ASM Action was set to None; *Custom Action* executed and undone by Undo Action button - ASM Action was set to None; *Custom Action* executed and undone by Timer - Action undone when *Custom Undo* executed by *Undo Action* button - Custom Action undone by Timer (Standard ASM Action set to None) - Custom Undo Action executed by *Undo Action* button (Standard ASM Action set to None) - Custom Undo Action executed by Timer (Standard ASM Action set to None) - Action undone by *Undo Action* button; *Custom Undo Action* failed - Action undone by Timer; *Custom Undo Action* failed - ASM Action set to None; *Custom Action* executed and *Custom Undo Action* failed - ASM Action set to None; and *Custom Undo Action* failed
Blank	No Action Taken	Action set to None

Icon	Status	Meaning
Blank	Custom Action Only	• ASM Action set to None; Custom action executed • ASM Action set to None; *Custom Action* failed **NOTE:** This status only appears when the ASM Action is set to *None*. Otherwise, the custom actions are noted in the Details column.
Blank	Port Excluded	• Port Type Filtered • Port Filtered
Blank	Search in Progress	Search began, but is not completed
Blank	Action in Progress	Action for this entry began, but is not completed.
Blank	Port Query in Progress	Port query began, but is not completed

Blank	Search Canceled	• Search canceled by *Cancel Search* menu option.
		• Operation Mode changed to Disabled while:
		  ◦ Search in Progress
		  ◦ Search Pending
		  ◦ Port Query in Progress
		  ◦ Port Query Pending
		• Console launched while:
		  ◦ Search in Progress
		  ◦ Search Pending
		  ◦ Port Query in Progress
		  ◦ Port Query Pending

Blank	Search Pending	Search for this entry is in the search queue.
Blank	Action Pending	Action for this entry is in the action queue.

Icon	Status	Meaning
Blank	Port Query Pending	Port query for this entry is in the port query queue.

Date/Time
: The date and time the incident is recorded in the Activity Monitor.

Sender ID

This is a unique identifier associated with the intrusion detection system that detected the security event.

Sender Name

The name associated with the intrusion detection system that detected the security event.

Event Category

The event category reported from the intrusion detection system. The following table lists the default categories.

ASM_ATTACK	ASM_COMPROMISE
ASM_INFORMATIONAL	ASM_MISUSE

Signature

This is a unique identifier, assigned to this attack by the intrusion detection system.

Threat IP

The IP address of the device that is the source of the threat (not the device on which the threat is detected).

Threat MAC

The MAC address of the device that is the source of the threat (not the device on which the threat is detected).

Device/Port

The IP address and port of the device where the initiator of the threat is detected.

Rule Name

The name of the action taken.

Action

This column describes the action configured for the rule (disable port, Apply Policy, No Action).

Details

This is brief (human-readable) description of the status for this incident. Refer to the Icon/Status descriptions for status information.

Last Updated

The timestamp for the previous action. This is the date and time when the last action is taken for this same event.

Filtered Traps

This is a count of the duplicate traps filtered. A trap is considered a duplicate if it has the same *Sender ID*, *Threat Category*, and *Threat IP Address* as an incident already in the Activity Monitor list. The trap is filtered if the incident in the Activity Monitor has a status of *Search Pending*.

Search Time (sec)

The amount of time in seconds ASM searches for the source of the threat.

Right-Click Menu

A right-mouse click on a column heading or anywhere in the table body (or a left-mouse click on the Table Tools button when visible in the upper left corner of the table) opens a popup menu that provides access to a set of Table Tools you can use to manage information in the table. In addition to these standard Table Tool options, the right-click menu can include the following:

- Incident Filter - Places the Incident Filter panel in the top half of the Activity Monitor window.
- Confirm Response - Confirms actions configured for **Manual Confirmation Required** in the Create Rule Window. This is an alternative to the **Confirm Response** button.
- Undo Action - Reverses the most recent action on the selected entries event/action in the Activity Monitor. This is an alternative to the **Undo Action** button. Refer to the description of the Undo Action button for more information on this option.
- Cancel Search - Causes the search for the selected entry to be terminated.
- View Details - Opens the **ASM Log Entry Details** window. The ASM Log Entry Details window provides additional information about the selected table entry(ies).

- **Delete Table Entry** - Removes the selected entries event/action in the Activity Monitor. This is an alternative to the **Delete Table Entry** button.

Buttons

Cancel Search

Aborts the currently pending search on the selected incident(s).

Confirm Response

This button confirms actions configured for **Manual Confirmation Required**. You can confirm a response in any operational mode (Search And Respond, Search Only, or Disabled).

When configuring an action that applies for a specific duration, the automatic undo remains suspended, even if the operational mode is set to Search and Respond. Refer to the Create/Edit Rule view for more information on this feature.

Undo Action

This button attempts to reverse the most recent action(s) on the selected entries in the Activity Monitor. When a Custom Undo Action is configured, this button executes the Custom Undo Action. Except for the situation noted below, only actions actually applied can be undone. For example, you cannot undo an action waiting confirmation.

NOTE: The exception can occur when two actions are defined, a standard ASM action and a custom action. If the standard ASM action fails, the custom action is applied and, if successful, cannot be undone. Under these circumstances, configure your custom action to take into account the potential failure of the standard ASM action.

Delete Table Entry

Removes the selected entries event/action in the Activity Monitor. When the entry removed is the last one for a particular incident, the associated Detail Log information is also deleted.

Clean Up Incidents

Opens the Clean Up Incidents window, where you can select incidents to delete from the Activity Monitor table.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Options Window
- Create/Edit Rule Window
- Log Entry Details

For information on related tasks:

- Getting Started with ASM
- How to Set Options
- How to Create/Edit ASM Rules

ASM Configuration Window

This feature lets you configure Automated Security Manager (ASM) to automatically respond to a variety of attacks on your network. ASM uses Extreme Networks Intrusion Prevention System (IPS) to identify threats to your network security and data integrity. Working with the NetSight database, an intrusion detection product (such as Extreme Networks IPS), and Policy Manager, ASM can identify a threat, locate its source, and automatically take action to isolate an offending port and mitigate a threat.

ASM is configured using the ASM Configuration Window. This window takes you step-by-step through configuring ASM actions and targets. The content of the ASM Configuration Window is dynamically updated as you set or change and define settings, always presenting the appropriate options based on your selections. As you move through the steps, the selections that you make along the way determine the appropriate selections for subsequent steps.

Common Features

Mode: View/Edit

Editing the configuration is only possible when the Configuration Window is set to **Edit**. Edit mode is only available to users that are members of an authorization group that has the **Manage Configuration** capability enabled. Refer to the Authorization/Device Access - Users and Groups Tab for more information.

Restore Defaults (Variable settings only)

Restores the default settings to the Variables in the ASM Configuration Window.

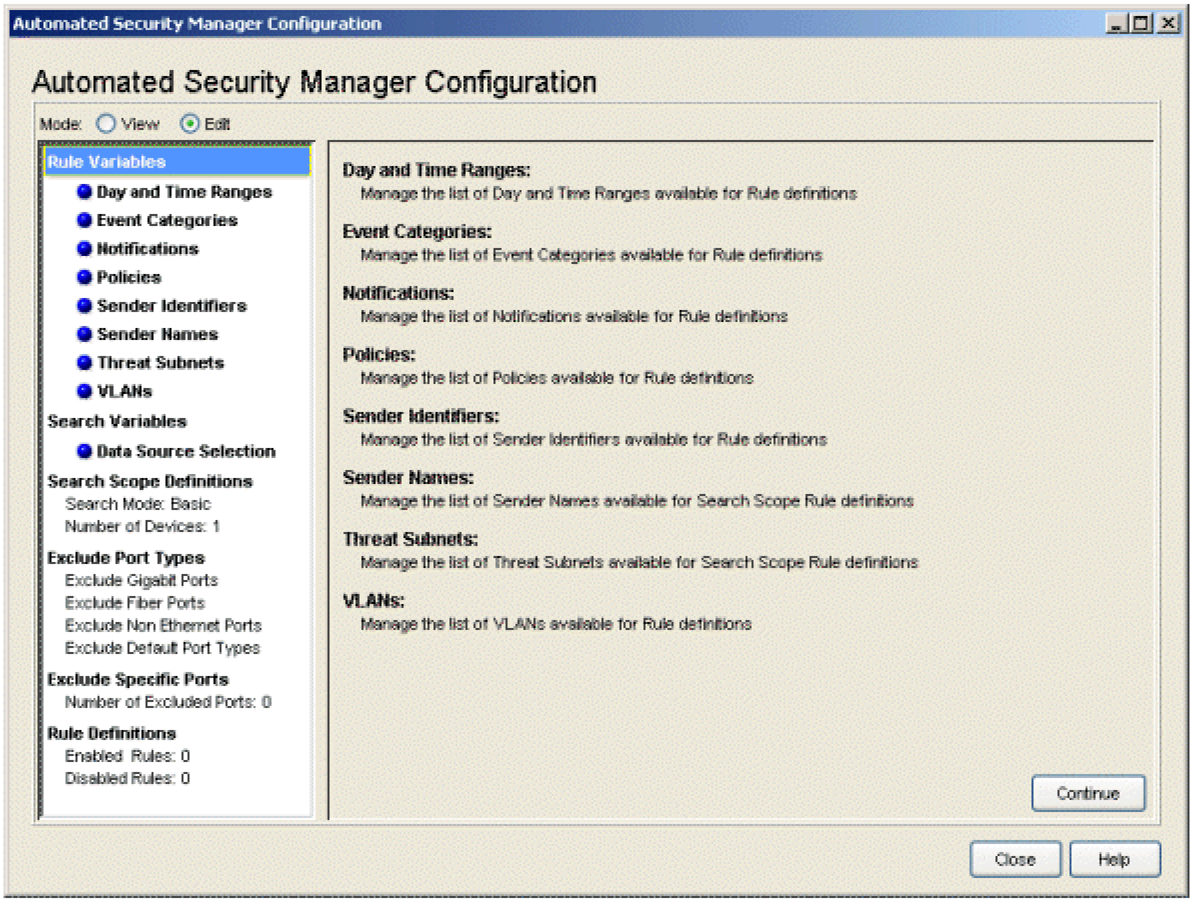
Continue/Save

At each step, click **Continue** to apply your settings and advance to the next configuration step. You can return to an earlier step by clicking any step in the left panel. At the final step,click **Save** to save the current rule definition.

Rule Variables

This section lets you define elements that can be matched by rules that determine when specific actions are applied. The **View/Edit** buttons above the left panel determine the ability to set or change the configuration in this window.

NOTE: The following Rule Variables views can be accessed from the ASM Configuration window or from the Qualifier Tabs in the Create Rule window.



Search Mode: Basic
Number of Devices: 1

Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Number of Excluded Ports: 0

Enabled Rules: 0
Disabled Rules: 0

Day and Time Ranges:
Manage the list of Day and Time Ranges available for Rule definitions

Event Categories:
Manage the list of Event Categories available for Rule definitions

Notifications:
Manage the list of Notifications available for Rule definitions

Policies:
Manage the list of Policies available for Rule definitions

Sender Identifiers:
Manage the list of Sender Identifiers available for Rule definitions

Sender Names:
Manage the list of Sender Names available for Search Scope Rule definitions

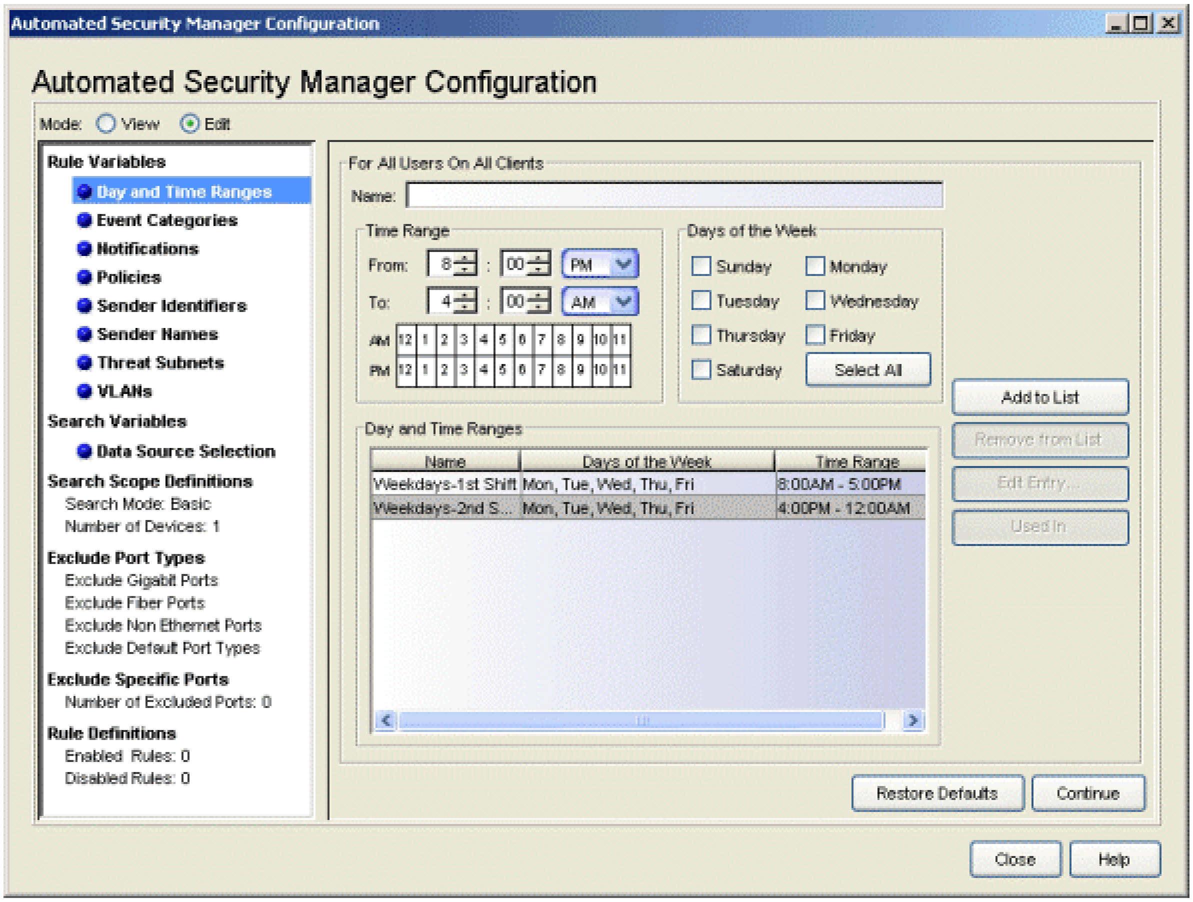
Threat Subnets:
Manage the list of Threat Subnets available for Search Scope Rule definitions

VLANs:
Manage the list of VLANs available for Rule definitions

Day and Time Ranges

This view lets you identify specific time intervals that may be pertinent when applying threat responses.

NOTE: The Day and Time Ranges view can be accessed from the ASM Configuration window (as shown below) or from the Qualifier Tabs in the Create Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables
- Data Source Selection

Search Scope Definitions
Search Mode: Basic
Number of Devices: 1

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 0
Disabled Rules: 0

For All Users On All Clients

Name:

Time Range
From: 8 : 00 PM
To: 4 : 00 AM

AM	12	1	2	3	4	5	6	7	8	9	10	11
PM	12	1	2	3	4	5	6	7	8	9	10	11

Days of the Week
□ Sunday □ Monday
□ Tuesday □ Wednesday
□ Thursday □ Friday
□ Saturday

Day and Time Ranges

Name	Days of the Week	Time Range
Weekdays-1st Shift	Mon, Tue, Wed, Thu, Fri	8:00AM - 5:00PM
Weekdays-2nd S...	Mon, Tue, Wed, Thu, Fri	4:00PM - 12:00AM

Name

The name of the time interval.

Time

Selects the time interval for this day and time range.

Days of the Week

Selects the days when the interval indicated in the **Time** field applies.

Day/Time Ranges

Displays defined Day/Time Ranges.

Select All/Deselect All

Selects all of the checkboxes in the Days of the Week area. When all days are selected, the button changes to a **Deselect All** button.

Add to List

Adds the current Days and Times definition to the Day/Time Ranges list.

Remove from List

Deletes a Days and Times definition selected in the Day/Time Ranges list.

Edit Entry

Opens the Edit Day/Time Entry window where you can adjust the current settings for a Days and Times definition selected in the Day/Time Ranges list.

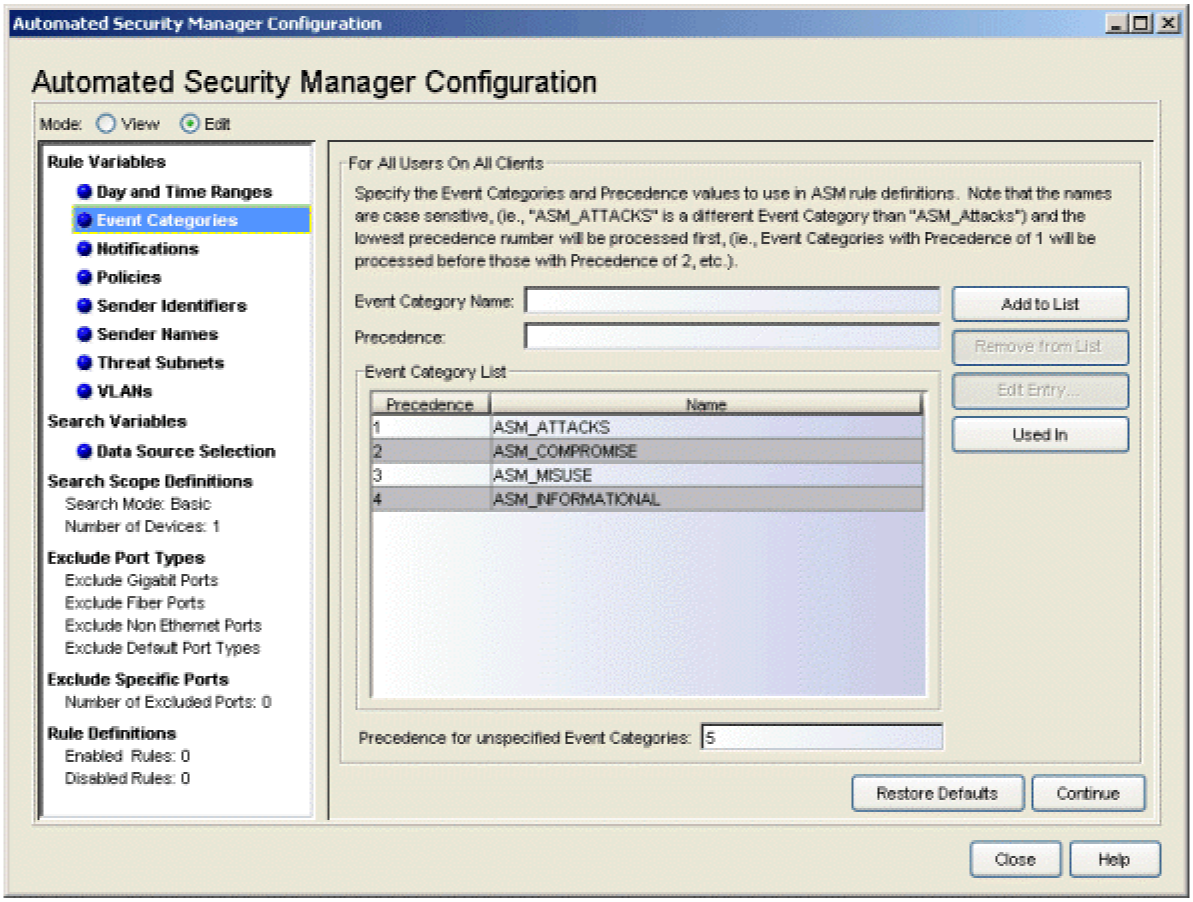
Used In

Select a Day/Time Range in the list, and click the **Used In** button to open a window that displays the ASM rules using the range.

Event Categories

This view lets you define the event categories that match events reported by an intrusion detection system. To be recognized by ASM, the text string in the event message sent by the IPS must match exactly the event category names here and in the Rule Definitions.

NOTE: The Event Category view can be accessed from the ASM Configuration window (as shown below) or from the Qualifier Tabs in the Create Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables
- Data Source Selection

Search Scope Definitions
Search Mode: Basic
Number of Devices: 1

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 0
Disabled Rules: 0

For All Users On All Clients

Specify the Event Categories and Precedence values to use in ASM rule definitions. Note that the names are case sensitive, (ie., "ASM_ATTACKS" is a different Event Category than "ASM_Attacks") and the lowest precedence number will be processed first, (ie., Event Categories with Precedence of 1 will be processed before those with Precedence of 2, etc.).

Event Category Name:

Precedence:

Event Category List

Precedence	Name
1	ASM_ATTACKS
2	ASM_COMPROMISE
3	ASM_MISUSE
4	ASM_INFORMATIONAL

Precedence for unspecified Event Categories: 5

Extreme Networks IPS has four default notification rules: netsight-atlas-asm-attacks, netsight-atlas-asm-compromise, netsight-atlas-asm-informational, and netsight-atlas-asm-misuse. Each of the notification rules has a corresponding event category in ASM: ASM_ATTACKS, ASM_COMPROMISE, ASM_INFORMATIONAL, and ASM_MISUSE.

For ASM's response to a serious threat to be timely and effective, it is important that ASM only be notified of serious threats. The following table lists the Extreme Networks IPS events for which notification to ASM is recommended:

BACKDOOR:PHATBOT	COMP:MS-DIR	COMP:ROOT-ICMP
COMP:ROOT-TCP	COMP:ROOT-UDP	COMP:SDBOT-LOGIN
COMP:SDBOT-NETINFO	COMP:SPYBOT-DOWNLOAD	COMP:SPYBOT-INFO
COMP:SPYBOT-KEYLOG	COMP:WIN-2000	COMP:WIN-XP
GENERIC:UPX-EXE	MS-BACKDOOR	MS-BACKDOOR2
MS-BACKDOOR3	MS-SQL:HAXOR-TABLE	MS-SQL:PWDUMP
MS-SQL:WORM-SAPPHIRE	MS:BACKDOOR-BADCMD	MS:BACKDOOR-DIR
SMB:SAMBAL-SUCCESS	SSH:HIGHPORT	SSH:X2-CHRIS
SSH:X2-CHRIS-REPLY		

Event Category List

This list contains all of the Event Categories defined for ASM. You can restore the default list by clicking **Restore Defaults**. The default event category and precedence settings are:

Precedence	Event Category	Precedence	Event Category
1	ASM_ATTACKS	2	ASM_COMPROMISE
3	ASM_MISUSE	4	ASM_INFORMATIONAL

Precedence

Precedence determines the order that ASM responds to certain Event Categories. A lower number yields a higher precedence, which means when multiple events are recognized, ASM responds to the highest precedence first. If all of the numbers are the same, then events are processed in the order they are received.

The Precedence values for the Default Event Categories are:

1. ASM_ATTACKS
2. ASM_COMPROMISE

3. ASM_MISUSE
4. ASM_INFORMATIONAL

Name

The name of the event category. Extreme Networks IPS has four default notification rules: netsight-atlas-asm-attacks, netsight-atlas-asm-compromise, netsight-atlas-asm-informational, and netsight-atlas-asm-misuse. Each of the default notification rules has a corresponding default event category in ASM: ASM_ATTACKS, ASM_COMPROMISE, ASM_INFORMATIONAL, and ASM_MISUSE. ASM uses Rules to compare incoming trap messages with specific event categories, then determines where and what action to apply as a response.

NOTE: Event Category names are case sensitive.

Precedence for unspecified Event Categories

If a threat is received that contains an Event Category not defined in the Event Category list, it is assigned the Precedence specified here. If you want to process all events according to the order they are received, set this value the same as the Precedence of all other Event Categories. If you want ASM to respond to these Event Categories first (since they are not expected and indicate an incorrect configuration on the network), set the Precedence to a lower number than all the others. If you want ASM to respond to these Event Categories last (since they are deemed to be the least important), set the Precedence to a higher number than all the others.

Add to List

Adds the Event Category, typed into the associated field, to the list.

Remove from List

Removes a selected Event Category from the list.

Edit Entry

Opens the Edit Event Category window where you can change the Name/Precedence for the selected Event Category.

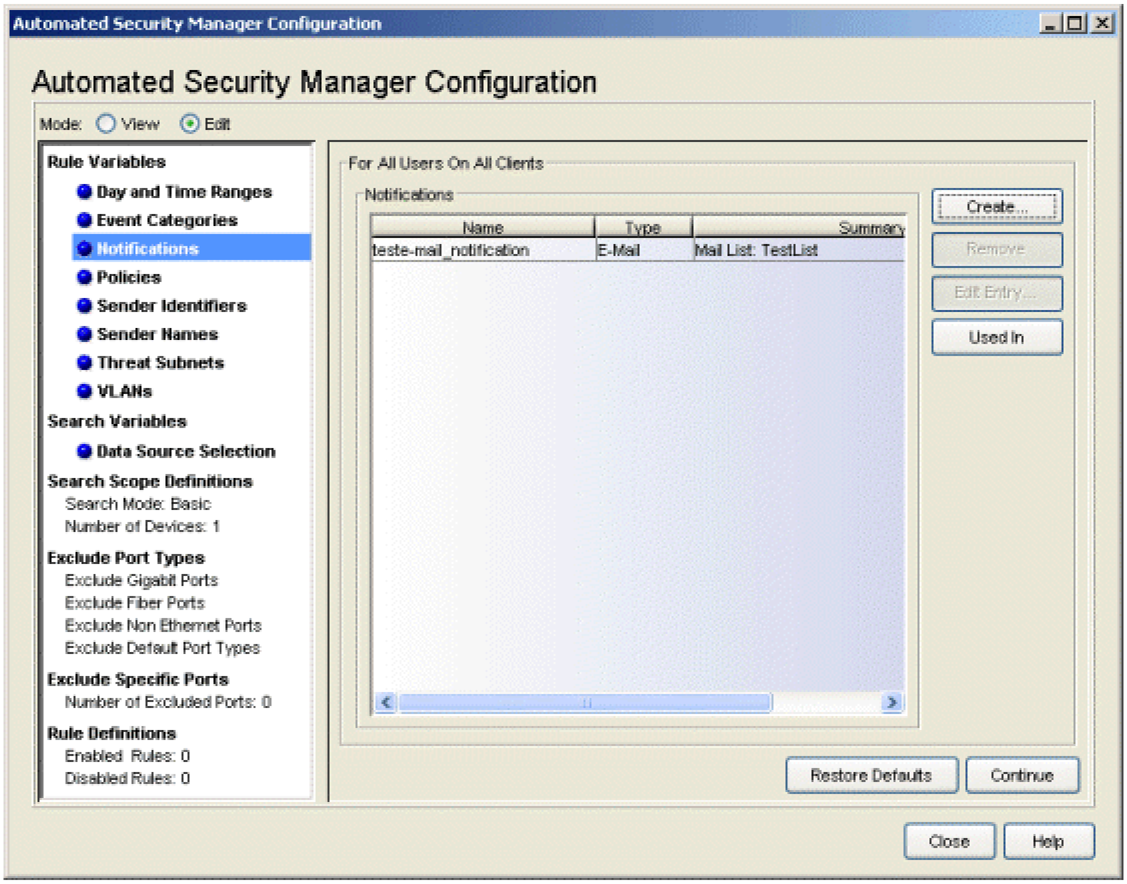
Used In

Select an Event Category in the list, and click the Used In button to open a window that displays the ASM rules using the category.

Notifications

This view lets you create, edit, and remove Notifications that can be activated together with a threat response. You can create notifications that send E-Mail, create a Syslog entry, trigger a SNMP trap, execute a script, or trigger a SNMP trap that is sent to Extreme Networks IPS. You can also combine two or more notifications into a group and treat that group as a single notification, thereby activating multiple notification types for a single event.

NOTE: The Notifications view can be accessed from the ASM Configuration window (as shown below) or from the Qualifier Tabs in the Create Rule window.



Automated Security Manager Configuration

Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables
- Data Source Selection

Search Scope Definitions
Search Mode: Basic
Number of Devices: 1

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 0
Disabled Rules: 0

For All Users On All Clients

Notifications

Name	Type	Summary
teste-mail_notification	E-Mail	Mail List: TestList

Notifications

This list shows all of the notifications created.

Create

Opens the Create Notification window. This window takes one of several forms, depending on the type of notification being created (E-Mail, Syslog, SNMP Trap, Script, Extreme Networks IPS, or Group).

Remove

Removes notifications selected in the Notifications list from the list. Notifications cannot be removed if they are currently in use by a rule. Attempting to remove a notification currently in use by a rule opens the Error removing Notification(s) window, which shows the rules where the selected notifications are used.

Edit Entry

Opens the Edit Notification window for a notification selected from the Notifications list. The specific form of Edit Notification window opened depends on the type of notification selected in the list (E-Mail, Syslog, SNMP Trap, Script, Extreme Networks IPS, or Group).

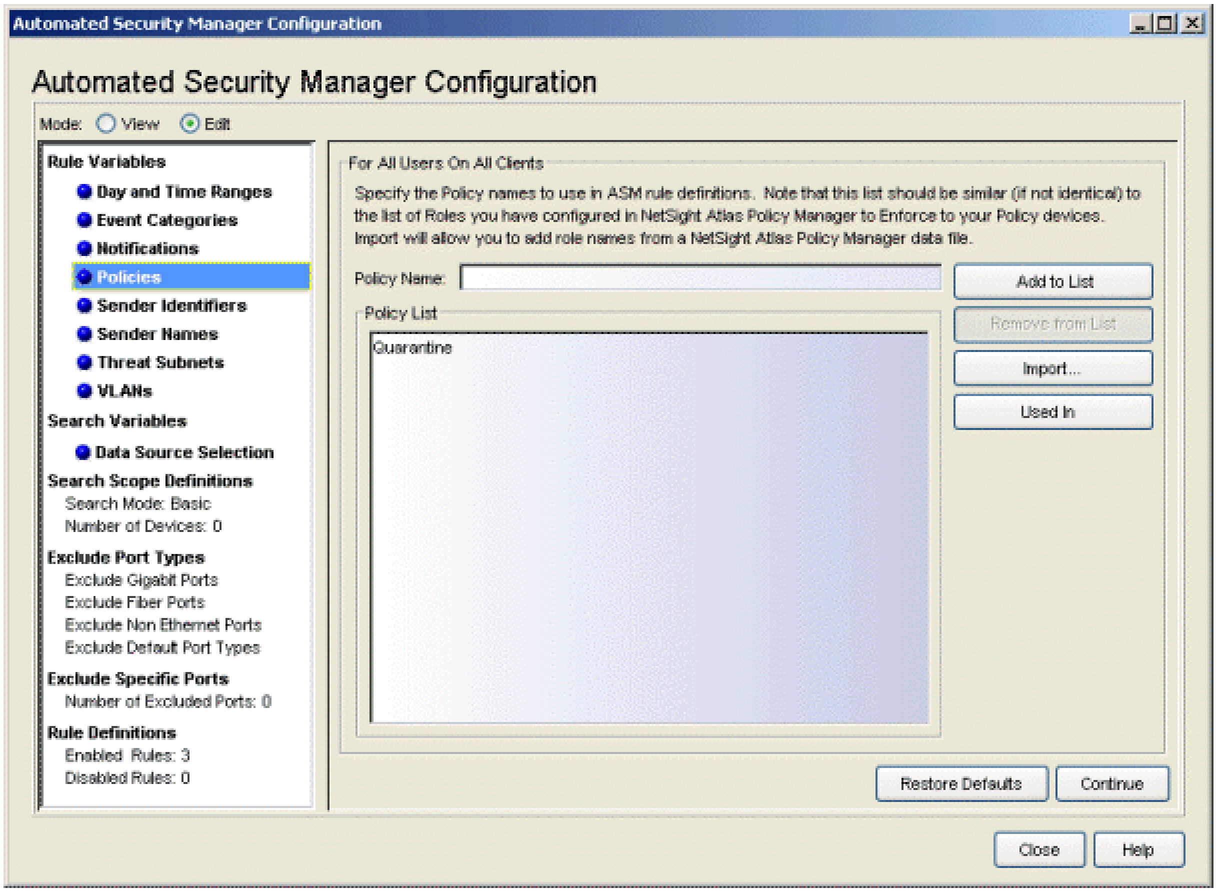
Used In

Select a Notification in the list, and click **Used In** to open a window that displays the ASM rules using the notification.

Policies

This view lets you add or remove Policies. Policies serve two purposes: they compare against roles currently applied to a port and they can also be applied as a response to a threat.

NOTE: The Policies view can be accessed from the ASM Configuration window (as shown below) or from the Qualifier Tabs in the Create Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables
- Data Source Selection

Search Scope Definitions
Search Mode: Basic
Number of Devices: 0

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 3
Disabled Rules: 0

For All Users On All Clients

Specify the Policy names to use in ASM rule definitions. Note that this list should be similar (if not identical) to the list of Roles you have configured in NetSight Atlas Policy Manager to Enforce to your Policy devices. Import will allow you to add role names from a NetSight Atlas Policy Manager data file.

Policy Name:

Policy List
Quarantine

Policy Name

The name of the Policy.

Policy List

Displays the Policies defined for ASM.

Add to List

Adds the Policy name, typed into the **Policy Name** field, to the list.

Remove from List

Removes the selected Policy from the list.

Import

Opens a file browser that allows you to select a .pmd file to import role names created in NetSight Policy Manager.

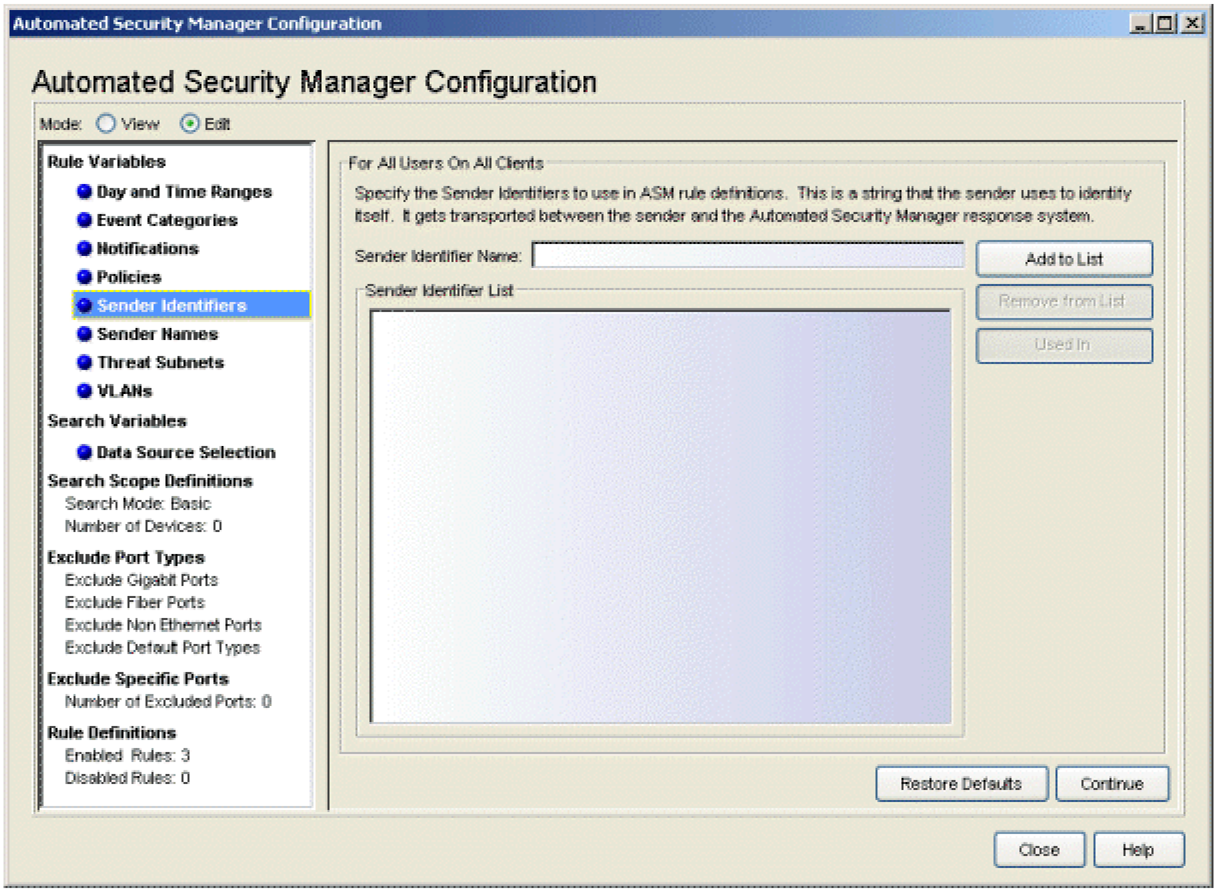
Used In

Select a Policy in the list, and click **Used In** to open a window that displays the ASM rules using the policy.

Sender Identifiers

This view lets you add or remove Sender Identifiers used to match events reported by an intrusion detection system.

NOTE: The Sender Identifiers view can be accessed from the ASM Configuration window (as shown below), from the Qualifier Tabs in the Create Rule window, or from the Rule Conditions section in the Create/Edit Search Scope Rule window.



Mode: ○ View ● Edit

Search Mode: Basic
Number of Devices: 0

Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Number of Excluded Ports: 0

Enabled Rules: 3
Disabled Rules: 0

Specify the Sender Identifiers to use in ASM rule definitions. This is a string that the sender uses to identify itself. It gets transported between the sender and the Automated Security Manager response system.

Sender Identifier Name:

NOTE: Sender Identifier names are case sensitive.

Sender Identifier Name

The name of the Sender Identifier.

Sender Identifier List

Displays the Sender Identifiers defined for ASM.

Add to List

Adds the Sender Identifier, typed into the associated field, to the list.

Remove from List

Removes the selected Sender Identifier from the list.

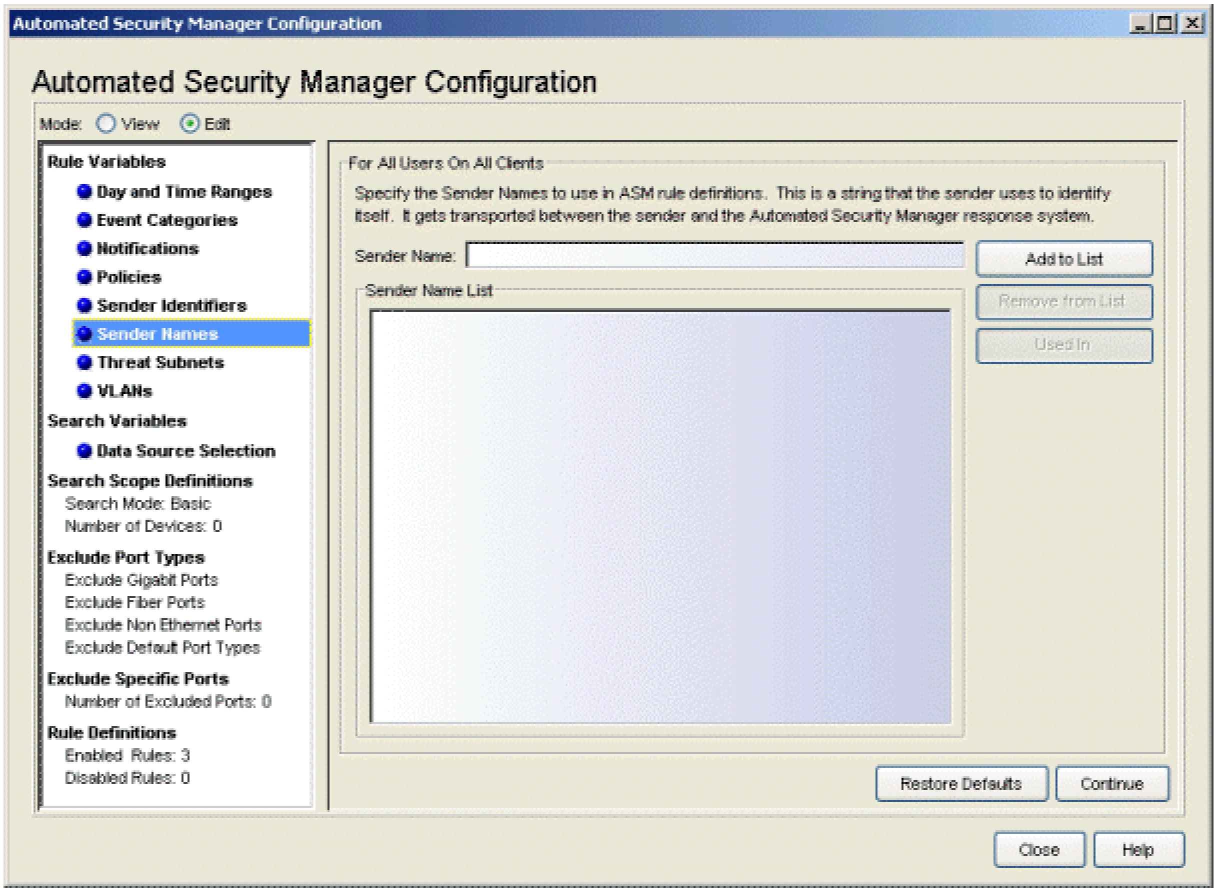
Used In

Select a Sender Identifier in the list, and click **Used In** to open a window displaying the ASM rules using the identifier.

Sender Names

This view lets you add or remove Sender Names used to define the ASM search scope when Extreme Networks IPS notifies ASM of a threat.

NOTE: The Sender Names view can be accessed from the ASM Configuration window (as shown below), from the Qualifier Tabs in the Create Rule window, or from the Rule Conditions section in the Create/Edit Search Scope Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

For All Users On All Clients

Specify the Sender Names to use in ASM rule definitions. This is a string that the sender uses to identify itself. It gets transported between the sender and the Automated Security Manager response system.

Sender Name:

Search Mode: Basic
Number of Devices: 0
Number of Excluded Ports: 0
Enabled Rules: 3
Disabled Rules: 0

NOTE: Sender Names are case sensitive.

Sender Name

The name of the Sender.

Sender Name List

Displays the Sender Names defined for ASM.

Add to List

Adds the Sender Name, typed into the associated field, to the list.

Remove from List

Removes a selected Sender Name from the list.

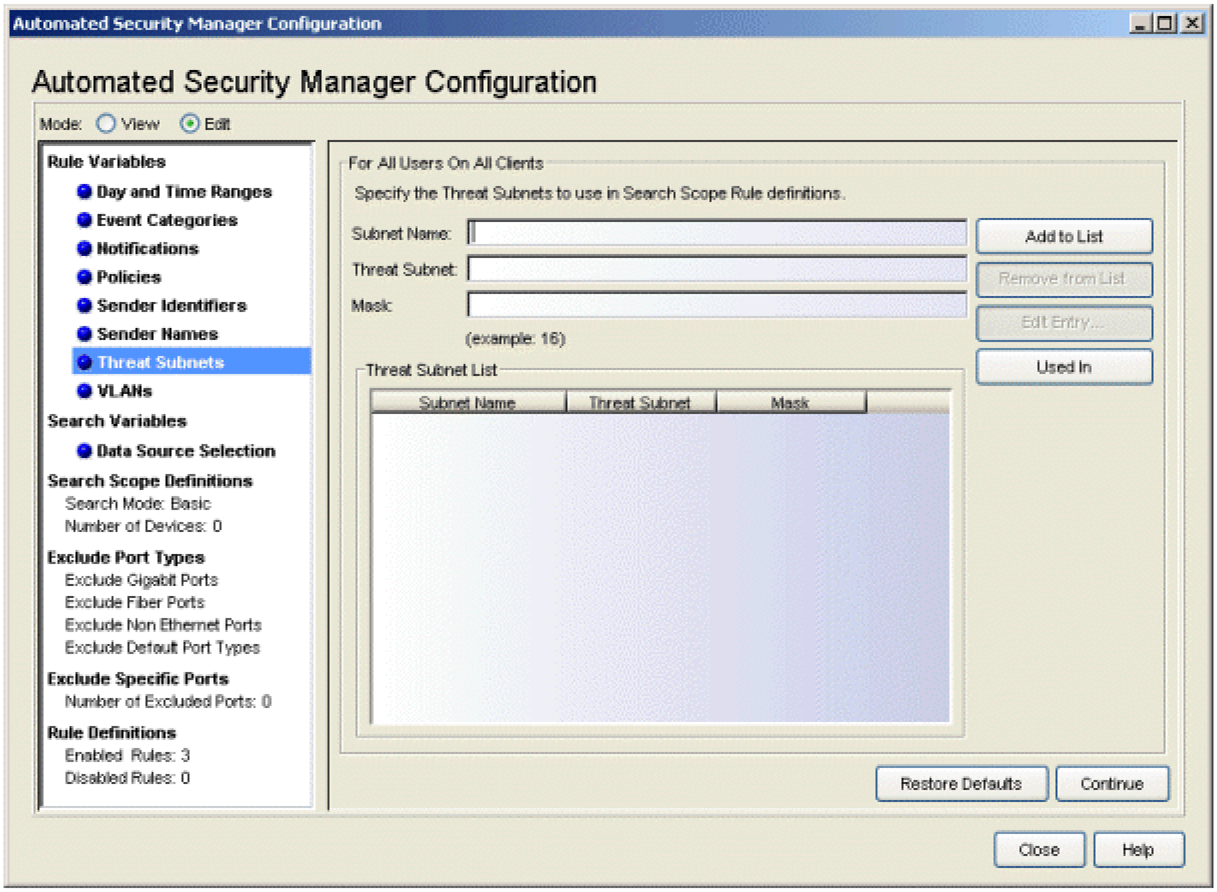
Used In

Select a Sender Name in the list, and **Used In** to open a window that displays the ASM rules using the name.

Threat Subnets

This view lets you add or remove subnets that define the ASM search scope when Extreme Networks IPS notifies ASM of a threat.

NOTE: The Threat Subnets view can be accessed from the ASM Configuration window (as shown below), from the Qualifier Tabs in the Create Rule window, or from the Rule Conditions section in the Create/Edit Search Scope Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Search Mode: Basic
Number of Devices: 0

Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Number of Excluded Ports: 0

Enabled Rules: 3
Disabled Rules: 0

Specify the Threat Subnets to use in Search Scope Rule definitions.

(example: 16)

Subnet Name

The name of the subnet.

Threat Subnet

The subnet the ASM search scope uses when Extreme Networks IPS notifies ASM of a threat.

Mask

The mask that further defines the associated subnet address. The format for the Mask is determined by the current **Network Mask** setting (CIDR or Dot-Delimited) selected in the Console Options - Data Display view.

Threat Subnet List

This list contains the Threat Subnets defined for ASM.

Add to List

Adds the Threat Subnet and Mask, typed into the associated fields, to the list.

Remove from List

Removes a selected Threat Subnet and Mask from the list.

Edit Entry

Opens the Edit Threat Subnet window where you can adjust the current settings for the selected Threat Subnet definition.

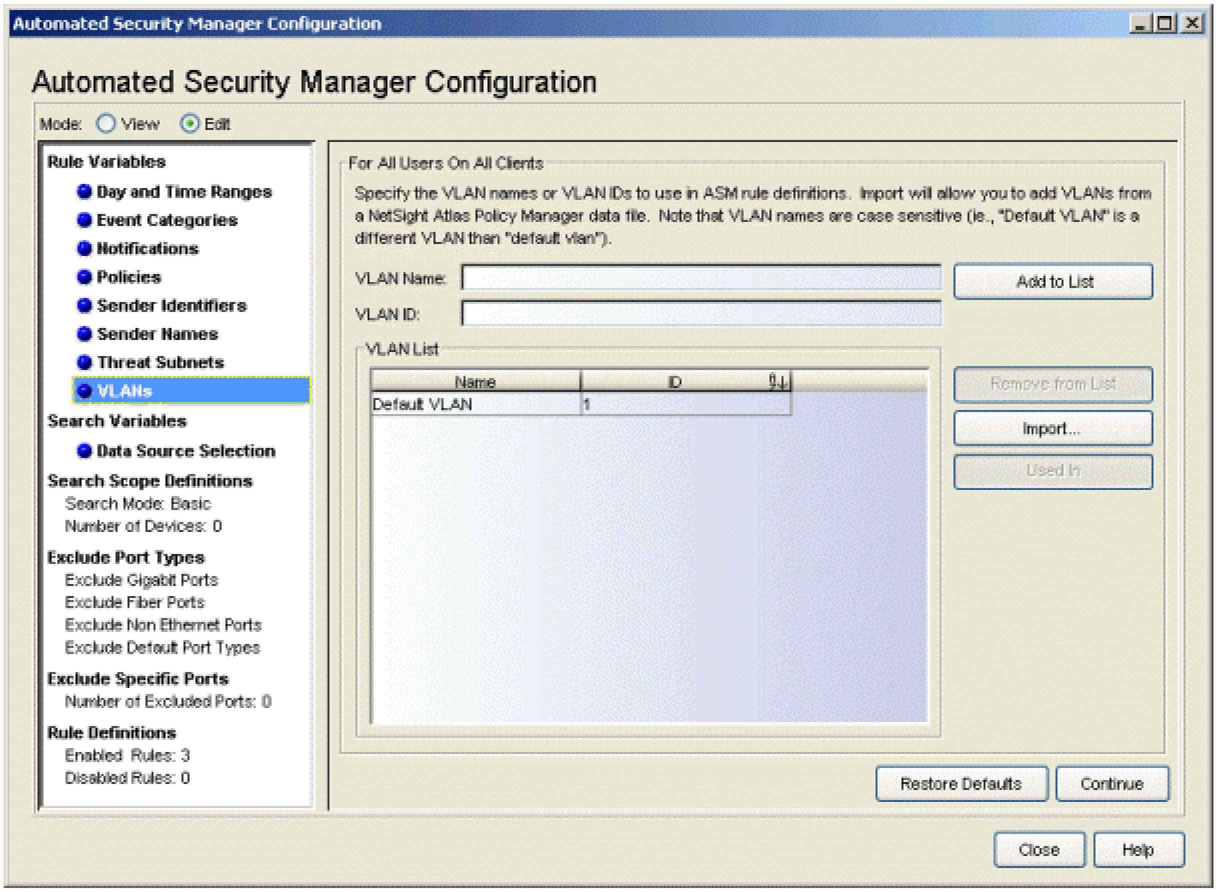
Used In

Select a Threat Subnet in the list and click **Used In** to open a window that displays the ASM rules using the subnet.

VLANs

This view lets you add or remove VLANs. VLANs serve two purposes. They are used to compare against roles currently applied to a port and they can also be applied as a response to a threat.

NOTE: The VLAN view can be accessed from the ASM Configuration window (as shown below) or from the Qualifier Tabs in the Create Rule window.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Search Mode: Basic
Number of Devices: 0

Number of Excluded Ports: 0

Enabled Rules: 3
Disabled Rules: 0

For All Users On All Clients

Specify the VLAN names or VLAN IDs to use in ASM rule definitions. Import will allow you to add VLANs from a NetSight Atlas Policy Manager data file. Note that VLAN names are case sensitive (ie., "Default VLAN" is a different VLAN than "default vlan").

VLAN Name:

VLAN ID:

VLAN List

Name	ID
Default VLAN	1

VLAN Name
: The VLAN name.

VLAN ID
: The VLAN ID.

VLAN List
: This list contains the VLANs defined for ASM.

Add to List
: Adds the VLAN Name/VLAN ID, typed into the associated field(s), to the list (VLAN names are limited to 32 characters).

Remove from List
: Removes a selected VLAN from the list.

Import
: Opens a file browser where you can select a .pmd file to role names created in NetSight Policy Manager.

Used In
: Select a VLAN in the list and click **Used In** to open a window that displays the ASM rules using the VLAN.

Search Variables

ASM lets you select specific sources to be used when searching for the source of network threats.

Data Source Selection

This view lets you select the data sources and MIB objects used to resolve the IP address to a MAC address. Refer to the MIB/Table Descriptions topic for information about specific MIB object and data source selections. The selection for data sources used with ASM are separate from the selection made for Compass in the **NetSight Console Options**.

At the bottom of the view, there is an option that determines the match behavior for Exclude rules. By default, each rule is processed in the order listed in the Rule Definitions panel and the first rule that matches determines the action taken for that port. The exception to this behavior is an IP address that matches an Exclude rule. In this case, ASM continues looking at the other rules within the search scope, even though there was a match. However, when the **Exclude Rule Abort Search When Matched** checkbox is selected, if a threat matches the

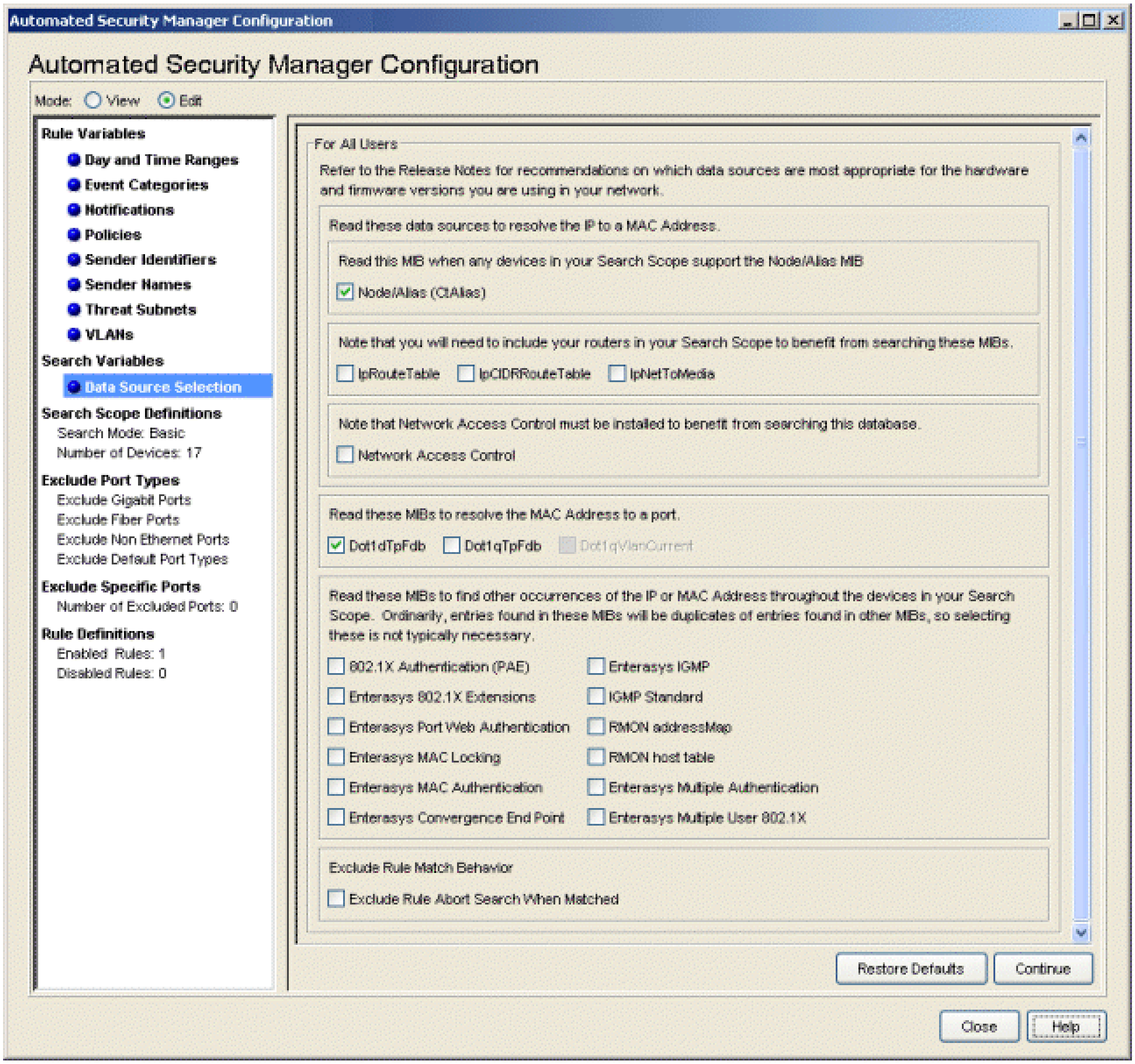
Exclude rule, ASM aborts the search and stops processing the additional rules looking for a legal search scope. If you select this option, verify the rules are listed in the appropriate order in the Rule Definition panel to prevent a search from aborting too soon.

Here is an example of the Exclude rule match behavior with and without the option enabled:

With a Threat IP Address of 10.2.222.2

Example Search Scope Rules:
Search Scope Rule 1: Exclude 10.2.222.0/23
Search Scope Rule 2: Match 10.2.0.0/16

With the option enabled, IP address 10.2.222.2 is within the excluded range of Rule 1. This causes the Search to abort.
With the option disabled, IP address 10.2.222.2 is not a match for Rule 1 and ASM continues to Rule 2 which is a match and starts the search.



Mode: ○ View ● Edit

Search Mode: Basic

Number of Devices: 17

Number of Excluded Ports: 0

Enabled Rules: 1

Disabled Rules: 0

For All Users

Refer to the Release Notes for recommendations on which data sources are most appropriate for the hardware and firmware versions you are using in your network.

Read these data sources to resolve the IP to a MAC Address.

Read this MIB when any devices in your Search Scope support the Node/Alias MIB

☑ Node/Alias (CtAlias)

Note that you will need to include your routers in your Search Scope to benefit from searching these MIBs.

□ IpRouteTable □ IpCIDRRouteTable □ IpNetToMedia

Note that Network Access Control must be installed to benefit from searching this database.

□ Network Access Control

Read these MIBs to resolve the MAC Address to a port.

☑ Dot1dTpFdb □ Dot1qTpFdb □ Dot1qVlanCurrent

Read these MIBs to find other occurrences of the IP or MAC Address throughout the devices in your Search Scope. Ordinarily, entries found in these MIBs will be duplicates of entries found in other MIBs, so selecting these is not typically necessary.

□ 802.1X Authentication (PAE) □ Enterasys IGMP
□ Enterasys 802.1X Extensions □ IGMP Standard
□ Enterasys Port Web Authentication □ RMON addressMap
□ Enterasys MAC Locking □ RMON host table
□ Enterasys MAC Authentication □ Enterasys Multiple Authentication
□ Enterasys Convergence End Point □ Enterasys Multiple User 802.1X

Exclude Rule Match Behavior

□ Exclude Rule Abort Search When Matched

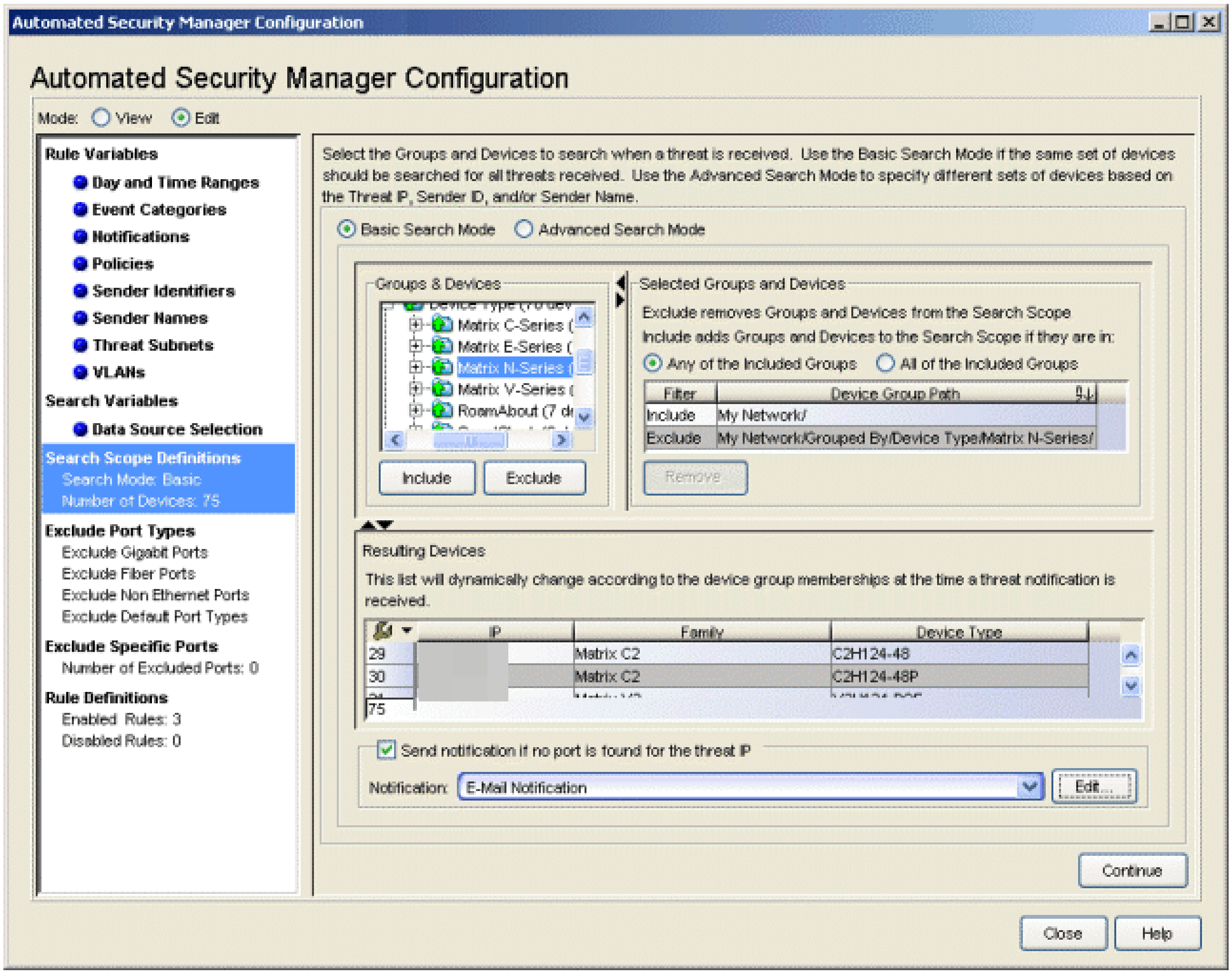
Search Scope Definitions

This view lets you select the devices searched when Extreme Networks IPS notifies ASM of a threat. You can set the search scope to **Basic** to create a single group to be searched or to **Advanced** to create more than one group of devices to search.

NOTE: ASM searches are performed by the NetSight Server, using the profile for the server, not the profile for the ASM client user.

Basic Search Scope

With **Basic Search Mode** selected the Search Scope Definitions view lets you include or exclude selected devices/device groups from a search to define the specific devices searched when Extreme Networks IPS notifies ASM of a threat. You can include or exclude specific devices, according to Device Type, Location, Contact, and Subnet.



Mode: ○ View ● Edit

Search Mode: Basic

Number of Devices: 75

Number of Excluded Ports: 0

Enabled Rules: 3

Disabled Rules: 0

Select the Groups and Devices to search when a threat is received. Use the Basic Search Mode if the same set of devices should be searched for all threats received. Use the Advanced Search Mode to specify different sets of devices based on the Threat IP, Sender ID, and/or Sender Name.

● Basic Search Mode ○ Advanced Search Mode

Exclude removes Groups and Devices from the Search Scope

Include adds Groups and Devices to the Search Scope if they are in:

● Any of the Included Groups ○ All of the Included Groups

Filter	Device Group Path
Include	My Network/
Exclude	My Network/Grouped By/Device Type/Matrix N-Series/

This list will dynamically change according to the device group memberships at the time a threat notification is received.

	IP	Family	Device Type
29	[redacted]	Matrix C2	C2H124-48
30	[redacted]	Matrix C2	C2H124-48P
75			

☑ Send notification if no port is found for the threat IP

Notification: E-Mail Notification Edit...

Groups & Devices

This panel shows the device tree for devices modeled in the Console database. You can expand branches of the tree to select Devices/Device Groups to be searched when Extreme Networks IPS notifies ASM of a threat. After making a selection, click **Include** to designate your selection(s) as being included in the search scope or click **Exclude** to designate your selection(s) as being specifically excluded in the search scope.

You can repeatedly select devices/device groups individually and click Include/Exclude or use multiple selection techniques (Control-click or Shift-Click) to select or deselect multiple Devices/Device Groups in a single operation.

NOTES:

1. When devices on your network do not support layer 3, include routers in the list of targets to allow ASM to use its IP to MAC address resolution feature to locate the end station. This includes the following devices:
   C3
   E1 (1G6xx Series)
   E5
   V-Series
   SS9000
   Vertical Horizong
   1st Generation 1HxxxSeries
2. ASM resolves IP addresses to MAC addresses using information from router MIBs (ipNetToMediaTable, ipNetToMediaTable, ipCidrRouteTable and ipRouteTable), but only if devices that can be modeled as a switch or a router are created in the Console database using the router's IP address. ASM cannot query information from the router MIBs unless devices are created using an IP address for the router interface.
3. Do **not** use Layer 3 NAC Controller and the NAC Gateway appliance as a search device in ASM. Configure ASM to search other devices in the network for the IP-to-MAC-to-port bindings, such as gateway routers for IP-to-MAC bindings and access edge switches for MAC-to-port information.

Selected Groups and Devices

This panel lists the devices/device groups selected from the Groups & Devices panel. The Filter column in the table indicates whether the device (s)/device group(s) can be included or excluded. The Device Group Path column shows the specific IP address and branch of the tree for selected devices/device groups.

Devices/device groups designated as Excluded are excluded from the search scope, regardless of any Include settings. For example, if a particular device is set to Excluded and the same device is a member of a device group that is set to Included, then the excluded device is not searched.

You can further refine your search scope by selecting either Any of the Included Groups or All of the Included Groups.

- **Any of the Included Groups** creates an OR condition such that if a selected device (not specifically excluded) is a member of any of the selected groups, then it is included in the search scope and appears in the Resulting Device/Device Group table. For example, selecting a specific Vertical Horizon device that is not in subnet 172.18.19.xx together with the *Vertical Horizon* and *IP Subnet 172.18,19.xx* Device Groups and clicking **Any of the Included Groups** includes all Vertical Horizon devices (including the individual VH device) and all devices from the 172.18,19.xx subnet.
- **All of the Included Groups** creates an AND condition. When selected, only devices that are members of all of the selected device groups are included in the search scope. This selection is useful when you want to select all of a particular device type, but only in a specific location--for example, all the routers in a particular building. When a device type (Routers) and a location group (Building2) are both selected, then only the devices contained in both groups (Routers in Building2) are included in the search scope.

Resulting Devices

The resulting list of devices searched when Extreme Networks IPS notifies ASM of a threat. The table is dynamically updated according to your device/device group selections and include/exclude arguments.

Send Notification...

This checkbox allows you to select a notification performed in the event no port is found for the Threat IP. For example, you can specify an E-Mail notification sent when no port is found. Select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window which lists the configured notifications. In this window, you can select a notification to edit, or click **Create** to open the Create Notification window.

Include/Exclude

Adds your tree selections to the Selected Groups and Devices table and sets the Filter column to either Include or Exclude.

Remove

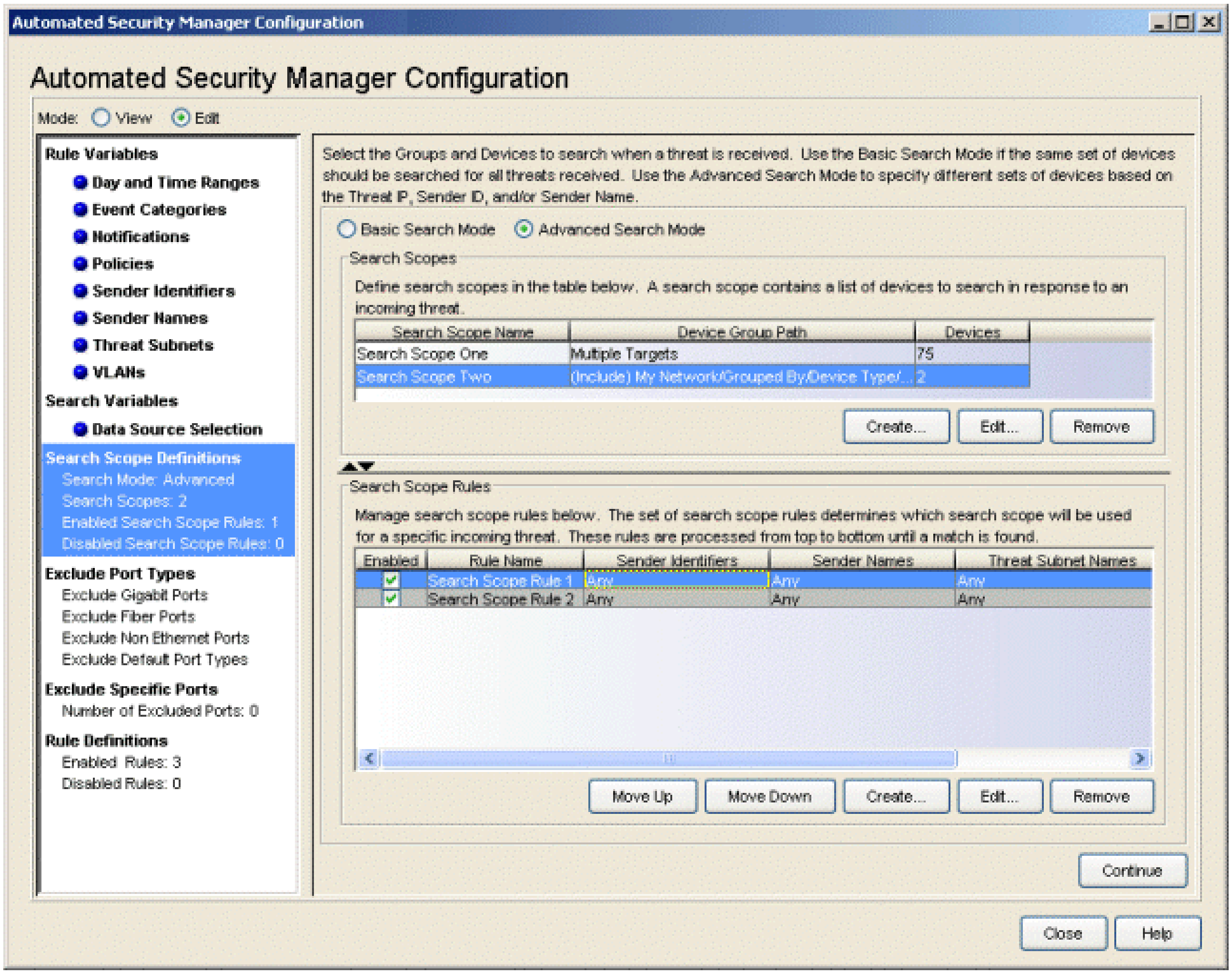
Deletes one or more rows selected from the **Groups and Devices** table.

Continue

Confirms the selected Devices/Device Groups and takes you to the **Exclude Port Types** view.

Advanced Search Scope

With **Advanced Search Mode** selected, the Search Scope Definitions view lets you create search scope rules to determine which devices to include or exclude from the ASM search when Extreme Networks IPS notifies ASM of a threat. Search Scope Rules are evaluated in order (from top-to-bottom) to examine the attributes of a threat (Sender ID, Sender Name and Sender Subnet) and when the threat matches the rule, the Search Scope Group associated with the rule is included in or excluded from the ASM search scope, according to the include/exclude arguments.



Automated Security Manager Configuration

Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- **Day and Time Ranges**
- **Event Categories**
- **Notifications**
- **Policies**
- **Sender Identifiers**
- **Sender Names**
- **Threat Subnets**
- **VLANs**

Search Variables
- **Data Source Selection**

Search Scope Definitions
Search Mode: Advanced
Search Scopes: 2
Enabled Search Scope Rules: 1
Disabled Search Scope Rules: 0

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 3
Disabled Rules: 0

Select the Groups and Devices to search when a threat is received. Use the Basic Search Mode if the same set of devices should be searched for all threats received. Use the Advanced Search Mode to specify different sets of devices based on the Threat IP, Sender ID, and/or Sender Name.

○ Basic Search Mode ● Advanced Search Mode

Search Scopes

Define search scopes in the table below. A search scope contains a list of devices to search in response to an incoming threat.

Search Scope Name	Device Group Path	Devices
Search Scope One	Multiple Targets	75
Search Scope Two	(Include) My Network/Grouped By/Device Type/...	2

Search Scope Rules

Manage search scope rules below. The set of search scope rules determines which search scope will be used for a specific incoming threat. These rules are processed from top to bottom until a match is found.

Enabled	Rule Name	Sender Identifiers	Sender Names	Threat Subnet Names
☑	Search Scope Rule 1	Any	Any	Any
☑	Search Scope Rule 2	Any	Any	Any

Search Scopes

This panel lists the Search Scopes associated with Search Scope Rules, which ultimately determine the devices searched when Extreme Networks IPS notifies ASM of a threat. You can add New Search Scopes using the

Create button or you can modify existing Search Scopes by selecting the Search Scope and clicking **Edit**.

Search Scope Rules

This panel lists the Search Scope Rules. The rules are evaluated in order (from top-to-bottom) and, when the attributes from a threat match the rule, the Search Scope associated with the rule determines the devices searched when Extreme Networks IPS notifies ASM of a threat. You can add New Search Scope Rules using the **Create** button or modify existing Search Scope Rules by clicking **Edit**. You acn adjust the order of rules by selecting a rule in the table and using the **Move Up**/**Move Down** buttons to change its position in the table.

Create (Group)

Opens the Create Search Scope Group window to create groups of devices searched when Extreme Networks IPS notifies ASM of a threat.

Edit (Group)

Select a Search Scope in the table and click **Edit** to open the Edit Search Scope Group window to edit the set of devices included in the group.

Move Up/Move Down

Search Scope Rules are evaluated from top to bottom in the order in which they appear in the table. These buttons allow you to arrange the order by selecting a particular rule and clicking **Move Up** or **Move Down** to move it to the desired position.

Create (Rule)

Opens the Create Search Scope Rule window to create rules that determine the search scope used when a specific threat is detected.

Edit (Rule)

Select a Search Scope Rule in the table and click **Edit** to open the Edit Search Scope Rule window to edit the conditions of that rule.

Remove

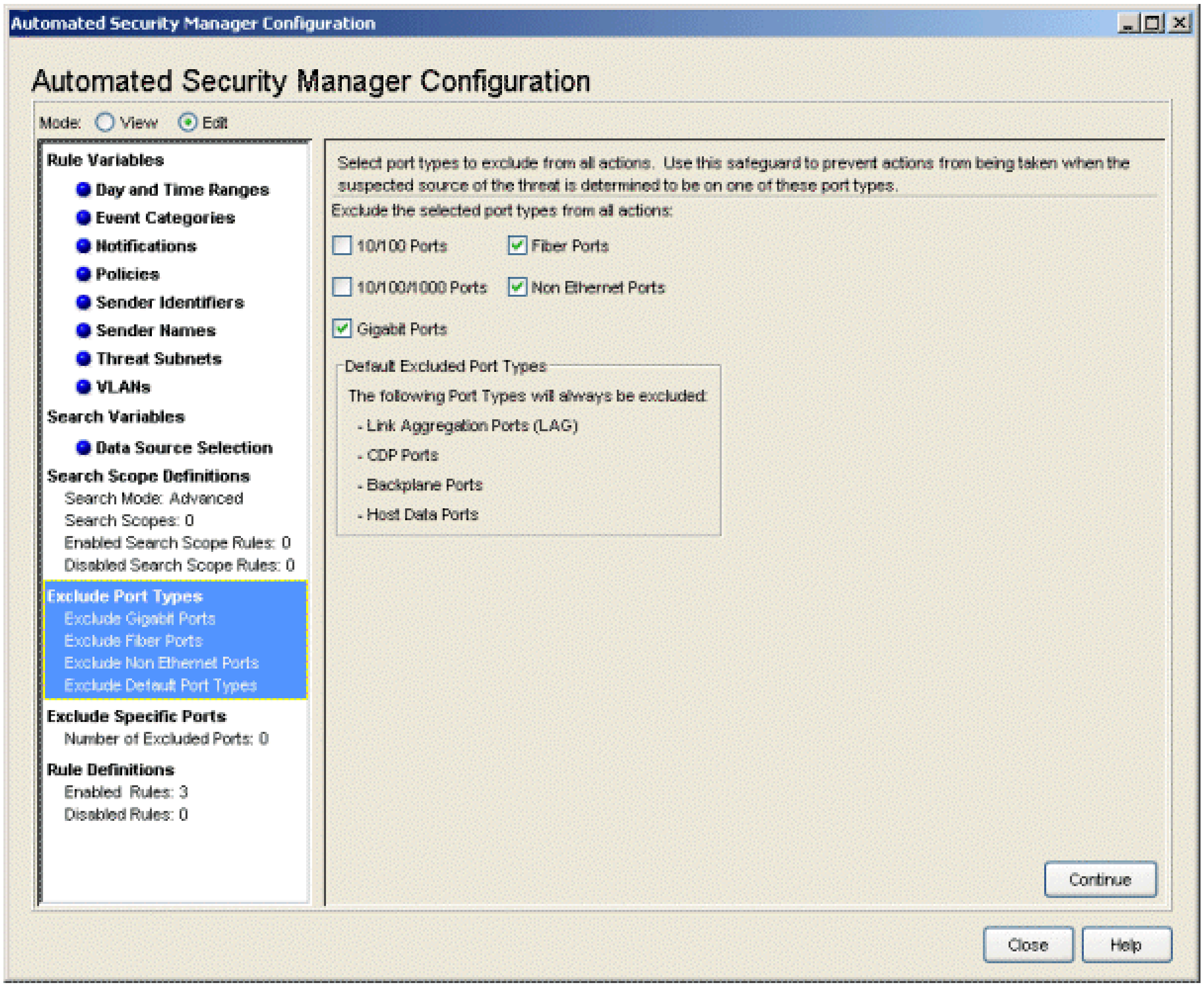
Deletes one or more rows selected from the associated table.

Continue

Confirms the defined Search Scopes and Search Scope Rules and takes you to the **Exclude Port Types** view.

Exclude Port Types

This view lets you exclude specific ports from threat management actions based on port type. This allows you to safeguard critical port types. Several check boxes list the port types available from the devices targeted for ASM actions. A check for a particular port type excludes that port type from threat management actions. Link Aggregation, CDP, Backplane, and Host Data ports are always excluded, by default.



Search Mode: Advanced
Search Scopes: 0
Enabled Search Scope Rules: 0
Disabled Search Scope Rules: 0

Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Number of Excluded Ports: 0

Enabled Rules: 3
Disabled Rules: 0

Select port types to exclude from all actions. Use this safeguard to prevent actions from being taken when the suspected source of the threat is determined to be on one of these port types.

Exclude the selected port types from all actions:

□ 10/100 Ports ☑ Fiber Ports

□ 10/100/1000 Ports ☑ Non Ethernet Ports

☑ Gigabit Ports

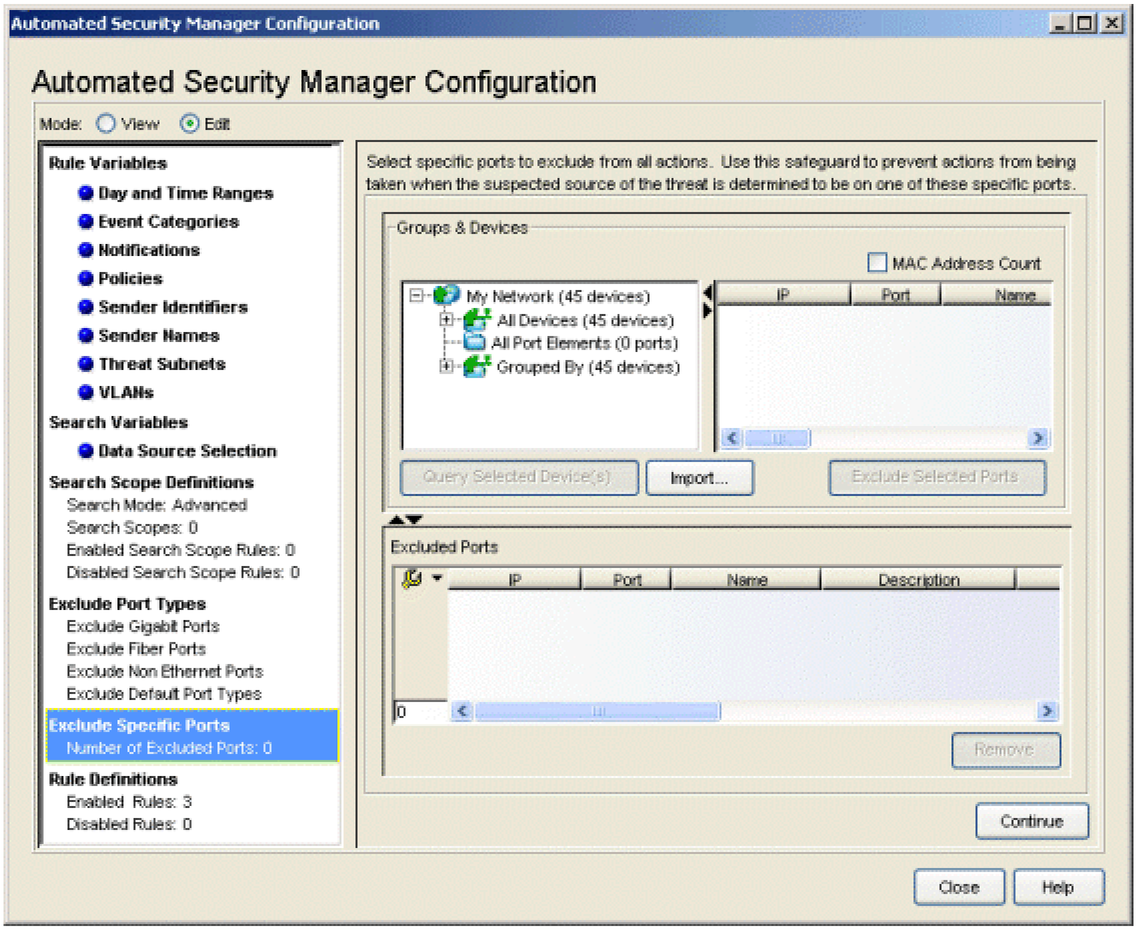
Default Excluded Port Types

The following Port Types will always be excluded:

- Link Aggregation Ports (LAG)
- CDP Ports
- Backplane Ports
- Host Data Ports

Exclude Specific Ports

This view lets you select specific ports to exempt from the actions by ASM to prevent shutting down critical ports.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables
- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables
- Data Source Selection

Search Scope Definitions
Search Mode: Advanced
Search Scopes: 0
Enabled Search Scope Rules: 0
Disabled Search Scope Rules: 0

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 3
Disabled Rules: 0

Select specific ports to exclude from all actions. Use this safeguard to prevent actions from being taken when the suspected source of the threat is determined to be on one of these specific ports.

□ MAC Address Count

MAC Address Count

This feature lets you distinguish between single-user ports and multi-user ports (routers). When checked, ASM expands its query to determine the number of MAC addresses connected through each port. The number of MAC addresses found appears in the **MAC Address Count** column of the **Groups and Devices** table.

Groups & Devices

The device tree shows the devices and port elements modeled in the Console database. Expand the tree to allow selecting one or more devices/port elements whose ports are excluded from ASM actions. Clicking **Query Selected Device(s)** displays the ports available on the devices in the table to the right of the tree.

Excluded Ports

This table lists the ports designated as exempt from the actions of ASM.

Query Selected Devices

Queries the Port Elements and device(s) selected in the tree to obtain a list of available ports.

Import

Opens a file browser to import a .pmd file from Policy Manager to exclude Frozen ports.

Exclude Selected Ports

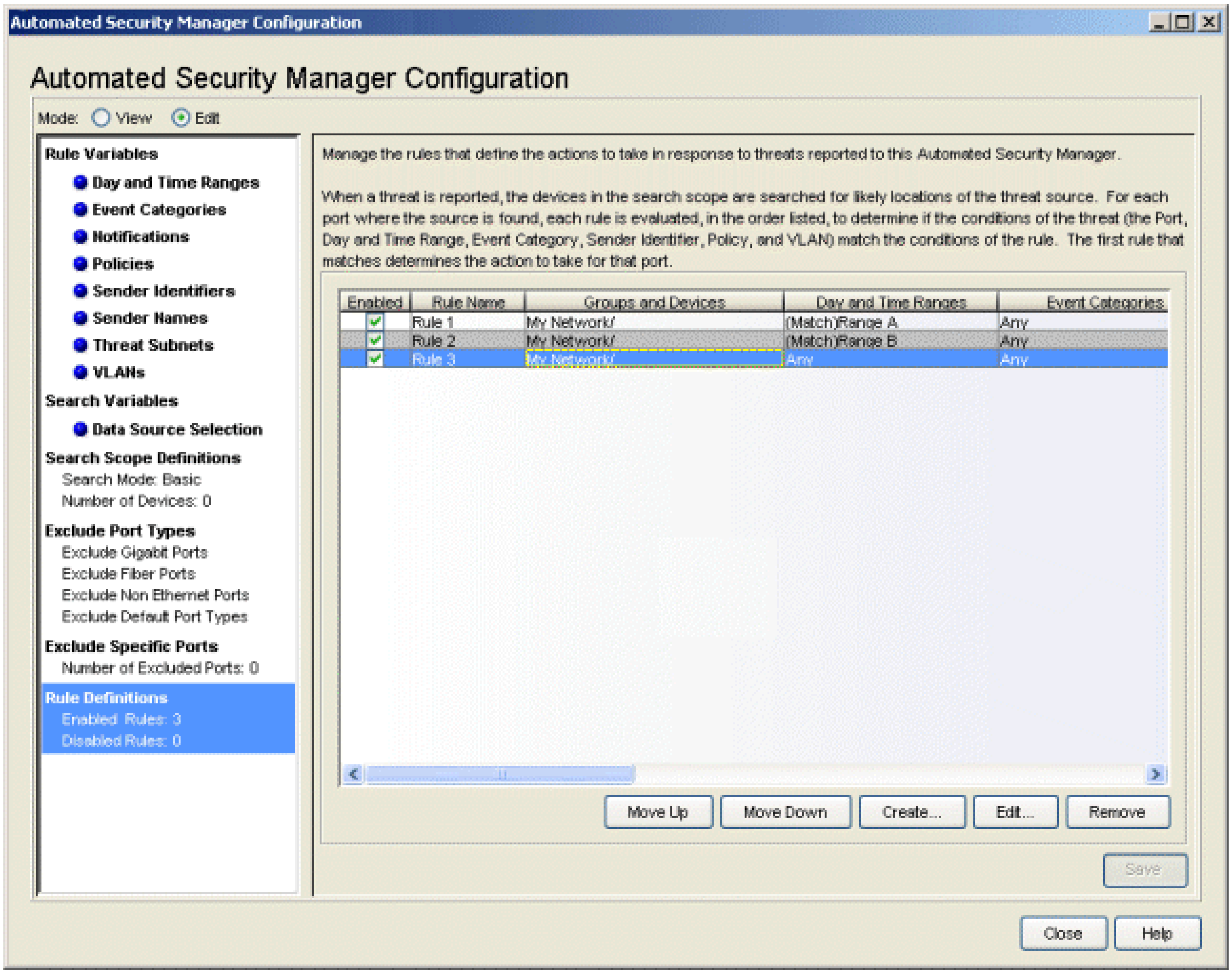
Adds the selected port(s) to the Excluded Ports table.

Remove

Removes port(s) selected in the Excluded Ports table.

Rule Definitions

This view lets you arrange the order of rules and enable or disable rules for the actions to be taken in response to intrusion threats. Upon notification of a trap from the intrusion detection system, the rules are executed from top to bottom, as they appear in the table. The Create button allows adding new rules to the table. The Edit button allows modifying an existing rule selected in the table.



Automated Security Manager Configuration

Mode: ○ View ● Edit

Rule Variables

- Day and Time Ranges
- Event Categories
- Notifications
- Policies
- Sender Identifiers
- Sender Names
- Threat Subnets
- VLANs

Search Variables

- Data Source Selection

Search Scope Definitions
Search Mode: Basic
Number of Devices: 0

Exclude Port Types
Exclude Gigabit Ports
Exclude Fiber Ports
Exclude Non Ethernet Ports
Exclude Default Port Types

Exclude Specific Ports
Number of Excluded Ports: 0

Rule Definitions
Enabled Rules: 3
Disabled Rules: 0

Manage the rules that define the actions to take in response to threats reported to this Automated Security Manager.

When a threat is reported, the devices in the search scope are searched for likely locations of the threat source. For each port where the source is found, each rule is evaluated, in the order listed, to determine if the conditions of the threat (the Port, Day and Time Range, Event Category, Sender Identifier, Policy, and VLAN) match the conditions of the rule. The first rule that matches determines the action to take for that port.

Enabled	Rule Name	Groups and Devices	Day and Time Ranges	Event Categories
☑	Rule 1	My Network/	(Match)Range A	Any
☑	Rule 2	My Network/	(Match)Range B	Any
☑	Rule 3	My Network/	Any	Any

Enabled

When checked, the action associated with the rule is executed in response to an intrusion threat.

Rule Name

This is the name assigned to the rule.

Groups and Devices

The devices/device groups on which a threat is suspected of ingressing the network.

Day and Time Ranges

The day and time ranges defined for the rule.

Event Categories

The event categories defined for the rule.

Sender Identifiers

The sender identifiers defined for the rule.

Policies

Port policies defined for this rule. Depending on how the rule is created, these policies may be overridden by the rule.

Action to Take

Identifies the action executed in response to the threat (**None**, **Apply Policy**, **Disable Port**, **Apply PVID**) when the rule matches the event criteria.

Confirmation

Indicates whether manual confirmation is required to execute the action.

Move Up/Move Down

Rules are executed from top to bottom in the order in which they appear in the table. These buttons allow you to arrange the order by selecting a particular rule and click **Move Up** or **Move Down** to move it to the desired position.

Create

Opens the Create Rule window where you can define a new rule to be added to the table.

Edit

Opens the Edit Rule window where you can modify an existing rule selected from the table.

Remove

Deletes a rule selected in the table.

Related Information

For information on related windows:

- Create/Edit Rule Window
- Options Window
- ASM Activity Monitor

For information on related tasks:

- How to Set Options
- How to Create and Edit Rules
- How to Use ASM Activity Monitor

ASM Options

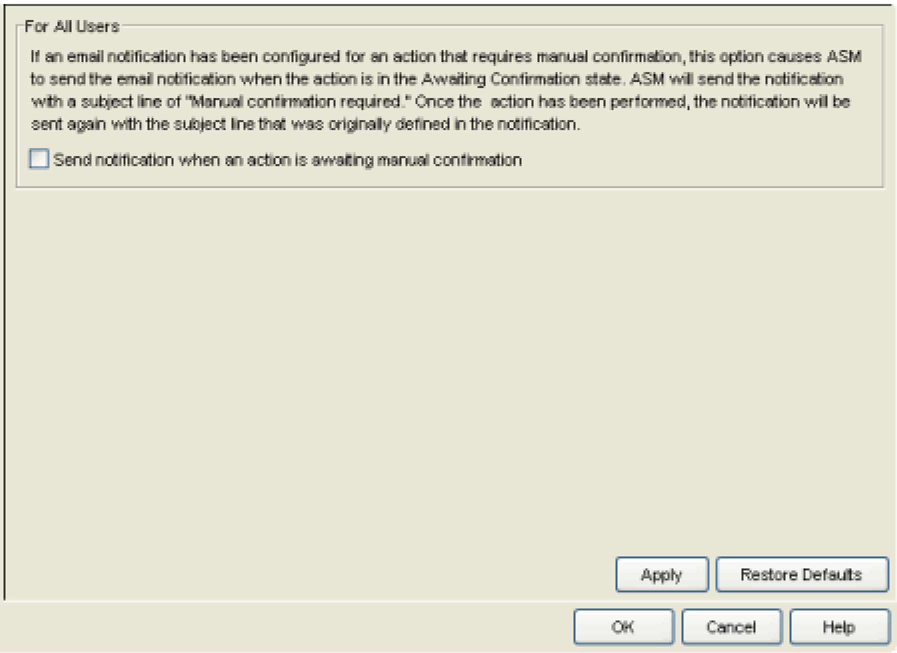
Automated Security Manager Options (**Tools > Options**) let you define your preferences for ASM operations. The right-panel view changes depending on what you have selected in the left-panel tree. Expand the Automated Security Manager folder to view all the different options you can set.

Information on the following ASM options:

- Advanced Settings
- Action Limits
- Dialog Boxes

Advanced Settings

If you have created a rule with an action that requires a manual confirmation before the action is taken, and an email notification has been configured for the action, ASM also sends an email notification when the action needs to be confirmed, if you select this option. The notification has a subject line of "Awaiting Manual Confirmation." Once you perform the action, the notification is sent again with the subject line originally defined in the notification. (Rule actions and notifications are configured in the Create Rule window.)



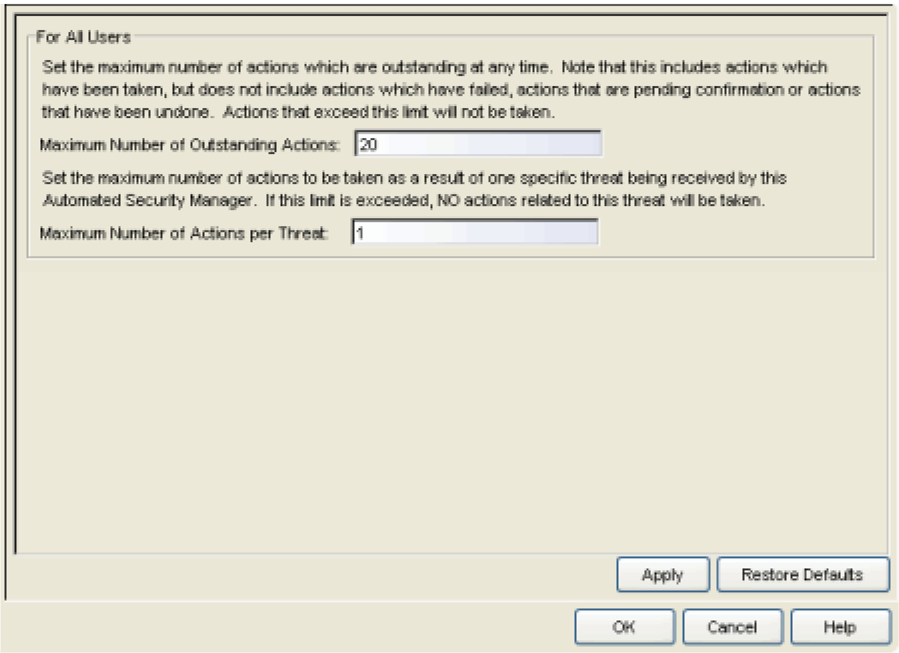
For All Users

If an email notification has been configured for an action that requires manual confirmation, this option causes ASM to send the email notification when the action is in the Awaiting Confirmation state. ASM will send the notification with a subject line of "Manual confirmation required." Once the action has been performed, the notification will be sent again with the subject line that was originally defined in the notification.

□ Send notification when an action is awaiting manual confirmation

Action Limits

This view lets you set limits for Automated Security Manager's threat responses.



For All Users

Set the maximum number of actions which are outstanding at any time. Note that this includes actions which have been taken, but does not include actions which have failed, actions that are pending confirmation or actions that have been undone. Actions that exceed this limit will not be taken.

Maximum Number of Outstanding Actions: 20

Set the maximum number of actions to be taken as a result of one specific threat being received by this Automated Security Manager. If this limit is exceeded, NO actions related to this threat will be taken.

Maximum Number of Actions per Threat: 1

Max Number of Outstanding Actions

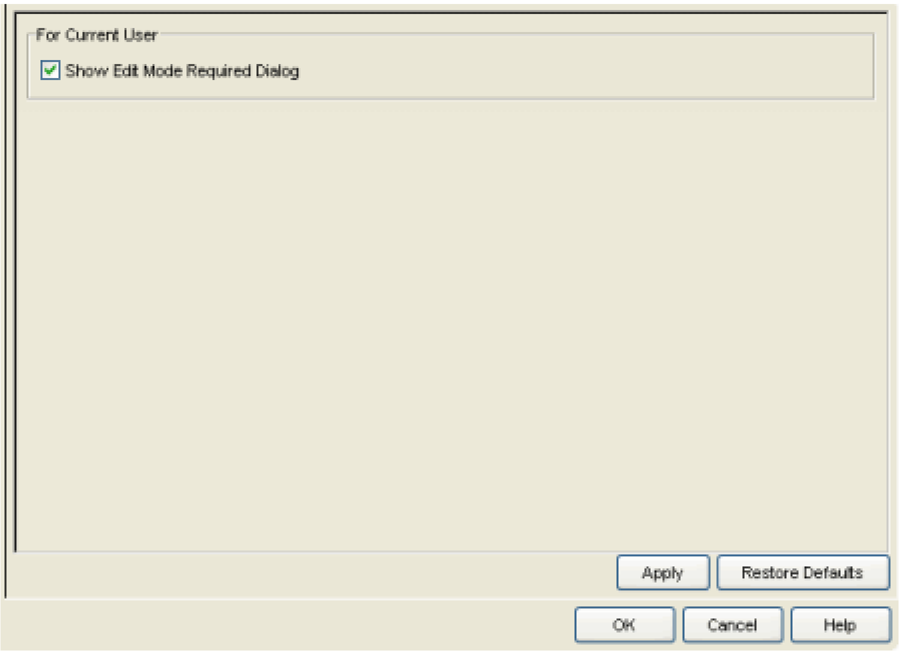
This parameter limits the number of outstanding (pending execution) actions.

Max Number of Action per Threat

This parameter sets a limit on the number of actions executed for a given threat. ASM counts both pending and executed actions toward the maximum. When the limit is reached, no further actions are executed for the threat.

Dialog Boxes

This view lets you configure whether certain dialog boxes are shown or ignored.



For Current User

☑ Show Edit Mode Required Dialog

Show Edit Mode Required Dialog

The Edit Mode Required dialog appears if you try to make changes in the ASM Configuration window without first selecting Edit Mode. Deselecting this checkbox means the dialog does not appear and you are automatically switched to Edit Mode.

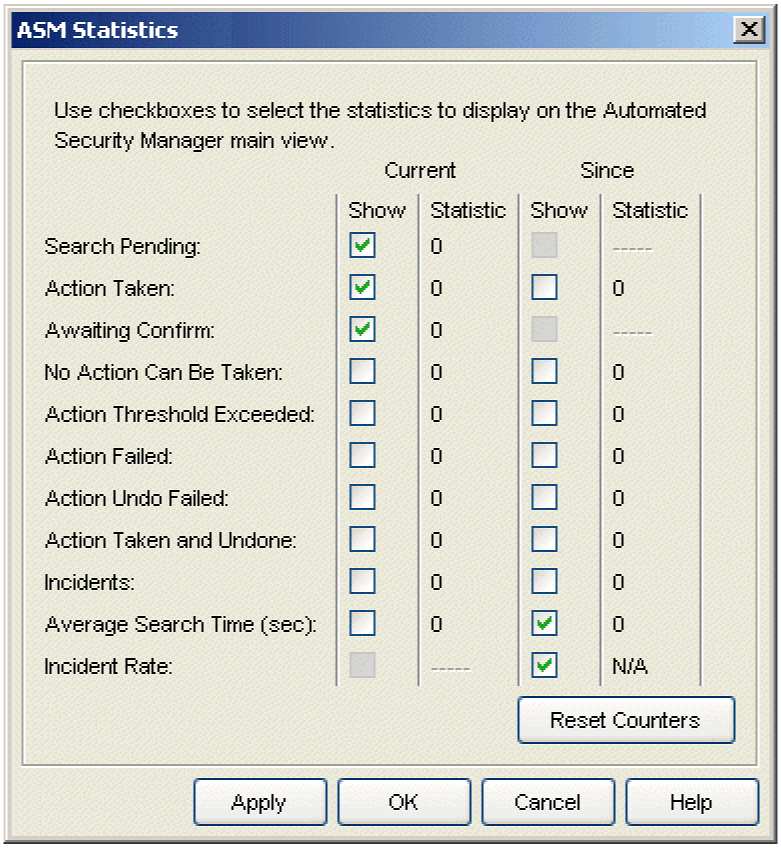
Related Information

For information on related windows:

- Automated Security Manager Activity Monitor
- Automated Security Manager Configuration Window
- Automated Security Manager - Create/Edit Rule Window

Select Statistics Window

This window lets you select the data elements that appear in the Statistics area of the ASM Activity Monitor window. It contains two sets of columns, one for Current statistics and another for Since statistics. Current statistics show the information about entries currently contained in the Activity Monitor table. Since statistics show the summation of information accumulated since the last counter reset. When checked, the associated data element appears in the Statistics area of the Activity Monitor.



Use checkboxes to select the statistics to display on the Automated Security Manager main view.

	Current		Since	
	Show	Statistic	Show	Statistic
Search Pending:	☑	0	□	------
Action Taken:	☑	0	□	0
Awaiting Confirm:	☑	0	□	------
No Action Can Be Taken:	□	0	□	0
Action Threshold Exceeded:	□	0	□	0
Action Failed:	□	0	□	0
Action Undo Failed:	□	0	□	0
Action Taken and Undone:	□	0	□	0
Incidents:	□	0	□	0
Average Search Time (sec):	□	0	☑	0
Incident Rate:	□	------	☑	N/A

Current

These statistics reflect the data currently contained in the Activity Monitor table.

Search Pending

The number entries in the table with a status of searches waiting to be performed.

Action Taken

The number entries in the table with a status of Action Taken.

Awaiting Confirm

The number entries in the table with a status of Awaiting Confirmation. These are entries for which rules are configured for manual confirmation.

No Action Can Be Taken

The number of entries in the table for which a standard or custom action cannot be taken.

Action Threshold Exceeded

The number of entries in the table that have exceeded the maximum number of actions per threat.

Action Failed

The number of entries in the table of standard or custom actions that failed.

Action Undo Failed

The number of entries in the table of standard or custom actions with an undo that failed.

Action Taken and Undone

The number of entries in the table of standard or custom actions taken that are undone by a timer or Undo Action button.

Incidents

The total number of incidents in the table.

Average Search time (sec)

For incidents in the table, the average time per incident spent searching.

Since

These statistics are an accumulation of data since the last time the counters were reset.

Action Taken

The number of times standard or custom action occurs successfully since the last reset.

No Action Can Be Taken

The number of times a standard or custom action could not be taken since the last reset.

Action Threshold Exceeded

The number of times the maximum number of actions per threat exceeded the defined threshold since the last reset.

Action Failed

The number of times a standard or custom action failed since the last reset.

Action Undo Failed

The number of times a standard or custom undo failed since the last reset.

Action Taken and Undone

The number of times a standard or custom action is taken and then undone by a timer or **Undo Action** button since the last reset.

Average Search time (sec)

The average time per incident spent searching since the last reset.

Incidents

The total number of incidents since the last reset.

Reset Counters

This button resets the counters for the accumulated data and sets the timestamp to the current date and time.

Related Information

For information on related windows:

- Automated Security Manager Options
- Automated Security Manager Activity Monitor

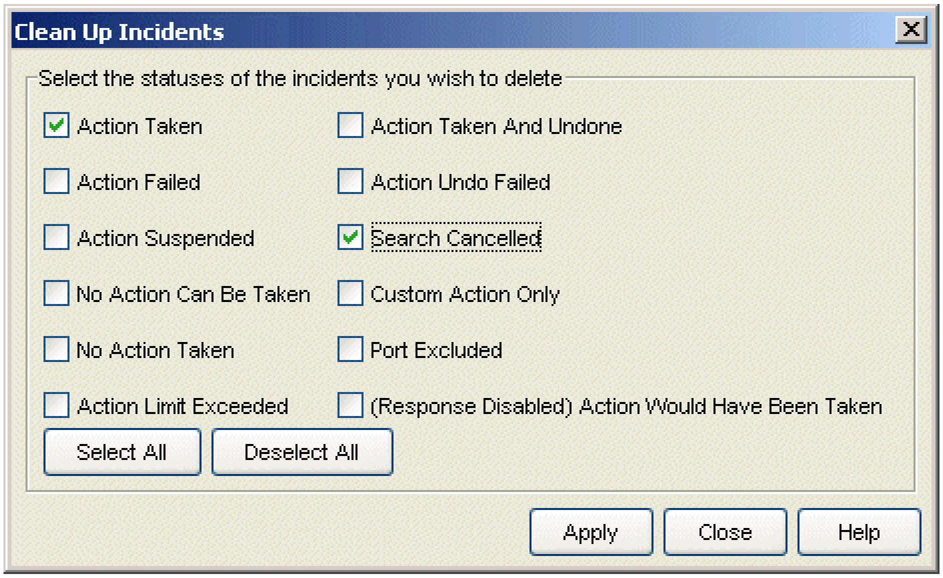
For information on related tasks:

- How to Set Automated Security Manager Options
- How to Use Automated Security Manager Activity Monitor

Clean Up Incidents Window

The Clean Up Incidents window lets you delete incidents from the Activity Monitor table based on incident status. Use the checkboxes to select the statuses of the incidents you want to delete. For more information on each status, see the Icon/Status section of the Activity Monitor Help topic.

The Clean Up Incidents window is accessed by clicking the **Clean Up Incidents** button in the Activity Monitor window.



Clean Up Incidents

Select the statuses of the incidents you wish to delete

☑ Action Taken
☐ Action Taken And Undone
☐ Action Failed
☐ Action Undo Failed
☐ Action Suspended
☑ Search Cancelled
☐ No Action Can Be Taken
☐ Custom Action Only
☐ No Action Taken
☐ Port Excluded
☐ Action Limit Exceeded
☐ (Response Disabled) Action Would Have Been Taken

Related Information

For information on related windows:

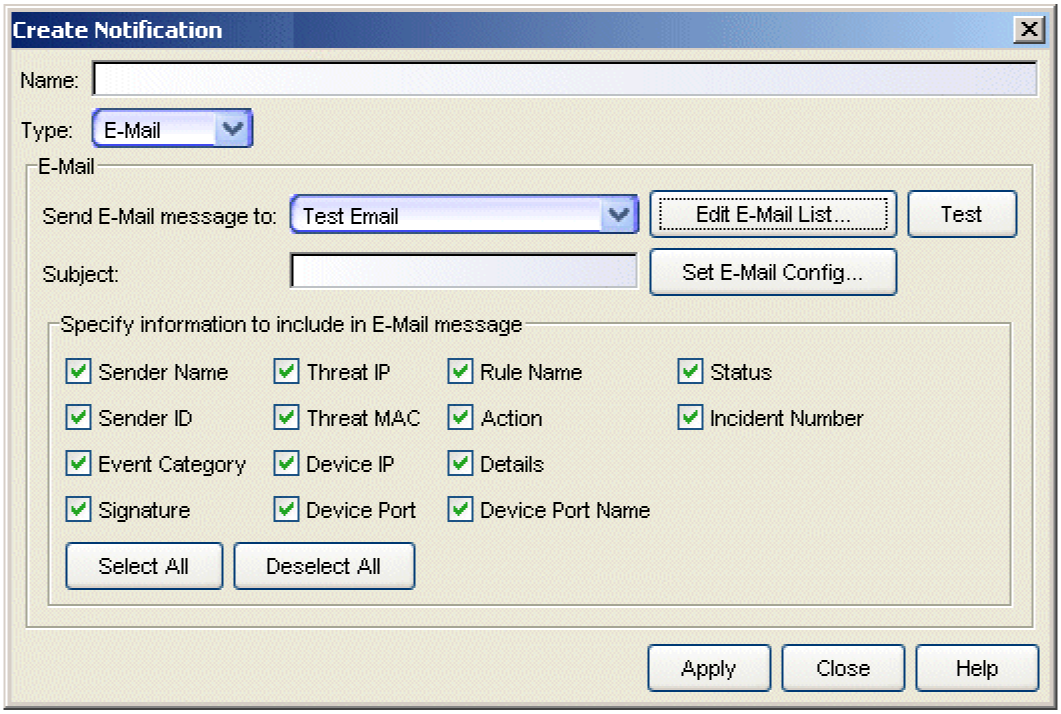
- ASM Activity Monitor

Create/Edit Notification Window

This window lets you create or edit notifications activated with your response to network threats. The window takes several forms depending on the type of notification being created or edited. Use the drop-down menu at the top of the window to select the type of notification you want to create. The appropriate fields are automatically provided.

E-Mail Notification

This window lets you configure E-Mail (message) notifications that trigger with your response to network threats.



Create Notification

Name:

Type: E-Mail

E-Mail

Send E-Mail message to: Test Email

Subject:

Specify information to include in E-Mail message

☑ Sender Name
☑ Sender ID
☑ Event Category
☑ Signature
☑ Threat IP
☑ Threat MAC
☑ Device IP
☑ Device Port
☑ Rule Name
☑ Action
☑ Details
☑ Device Port Name
☑ Status
☑ Incident Number

Name

The name assigned to this notification.

Type

Set the Type to E-Mail for this window.

Send E-Mail message to:

Use this drop-down menu to select one of your pre-defined E-Mail lists. If no lists have been defined, the menu is empty. Click the Edit E-Mail List button to define a list.

Subject

Enter the subject for the notification E-Mail message here.

Set E-Mail Config

This button opens the Options - SMTP E-Mail Server view, where you can specify an Outgoing SMTP E-Mail Server and a Sender address that appears as the sender in E-Mail notifications.

Specify information to include in E-Mail message

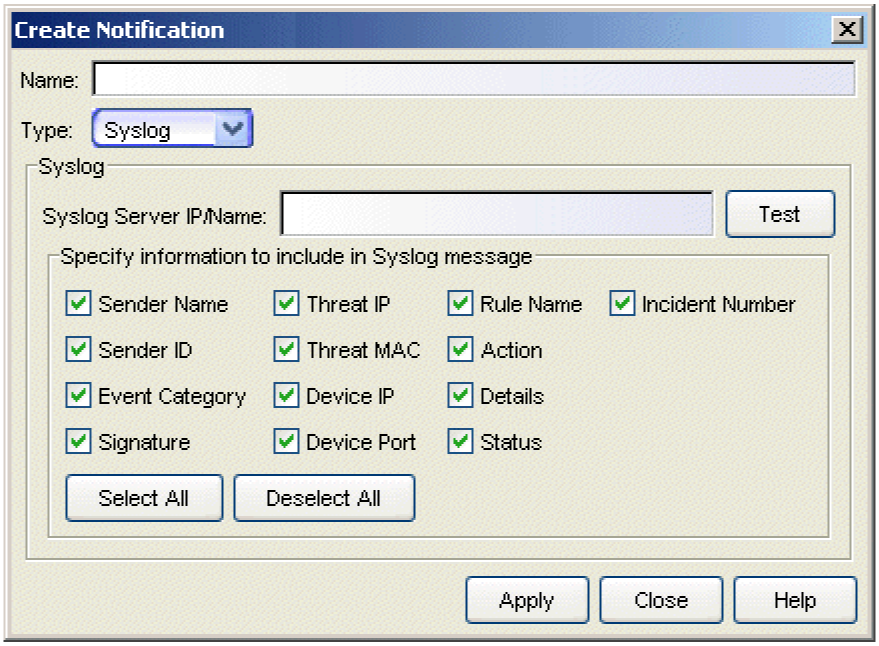
These check boxes let you select elements of the event information that are added to your E-Mail notification message. The **Select All** button places a check in all of the boxes and the **Deselect All** button removes checks from all of the boxes. The information is added to your message as unformatted, space-delimited text.

Test

This button allows sending a test message to simulate a notification sent in response to a network threat.

Syslog

This window lets you configure notifications to create a Syslog entry.



Create Notification

Name:

Type: Syslog

Syslog

Syslog Server IP/Name:

Specify information to include in Syslog message

☑ Sender Name ☑ Threat IP ☑ Rule Name ☑ Incident Number

☑ Sender ID ☑ Threat MAC ☑ Action

☑ Event Category ☑ Device IP ☑ Details

☑ Signature ☑ Device Port ☑ Status

Name

The name assigned to this notification.

Type

Set the Type to Syslog for this window.

Syslog Server IP/Name

This is the IP address or hostname that identifies the Syslog server where the message is sent.

Specify information to include in Syslog message

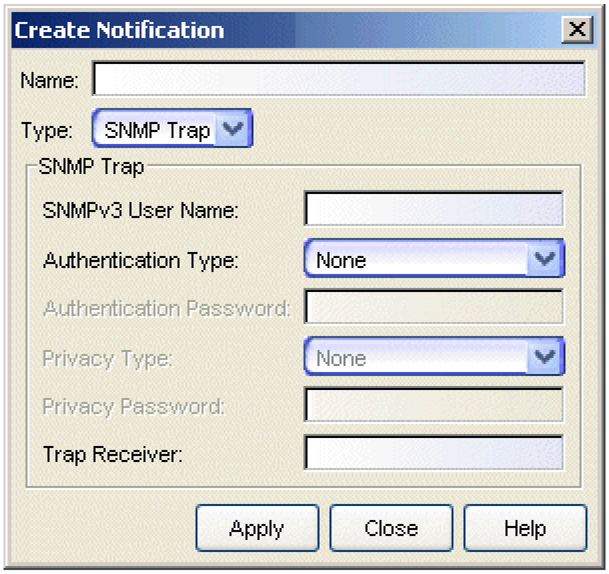
These checkboxes let you select elements of the event information to add to your Syslog notification message. The **Select All** button places a check in all of the boxes and the **Deselect All** button removes checks from all of the boxes. The information is added to your message as unformatted, space-delimited text.

Test

This button allows sending a test syslog message to simulate a notification sent in response to a network threat.

SNMP Trap

This window lets you configure notifications that send a SNMP Trap triggered with your response to network threats.



Create Notification

Name:

Type: SNMP Trap

SNMP Trap

SNMPv3 User Name:

Authentication Type: None

Authentication Password:

Privacy Type: None

Privacy Password:

Trap Receiver:

Name

The name assigned to this notification.

Type

Set the Type to SNMP Trap for this window.

SNMPv3 User Name

This is the user name for the credential used when sending the trap to the Trap Receiver.

Authentication Type

MD5 or **SHA1** or **None**, selected from this drop-down menu.

Authentication Password

This is the password (between 1 and 64 characters in length) used to determine Authentication. This field is disabled if Authentication Type is **None**.

Privacy Type

Select **DES** or **None** from this drop-down menu. These settings are disabled if Authentication Type is **None**.

Privacy Password

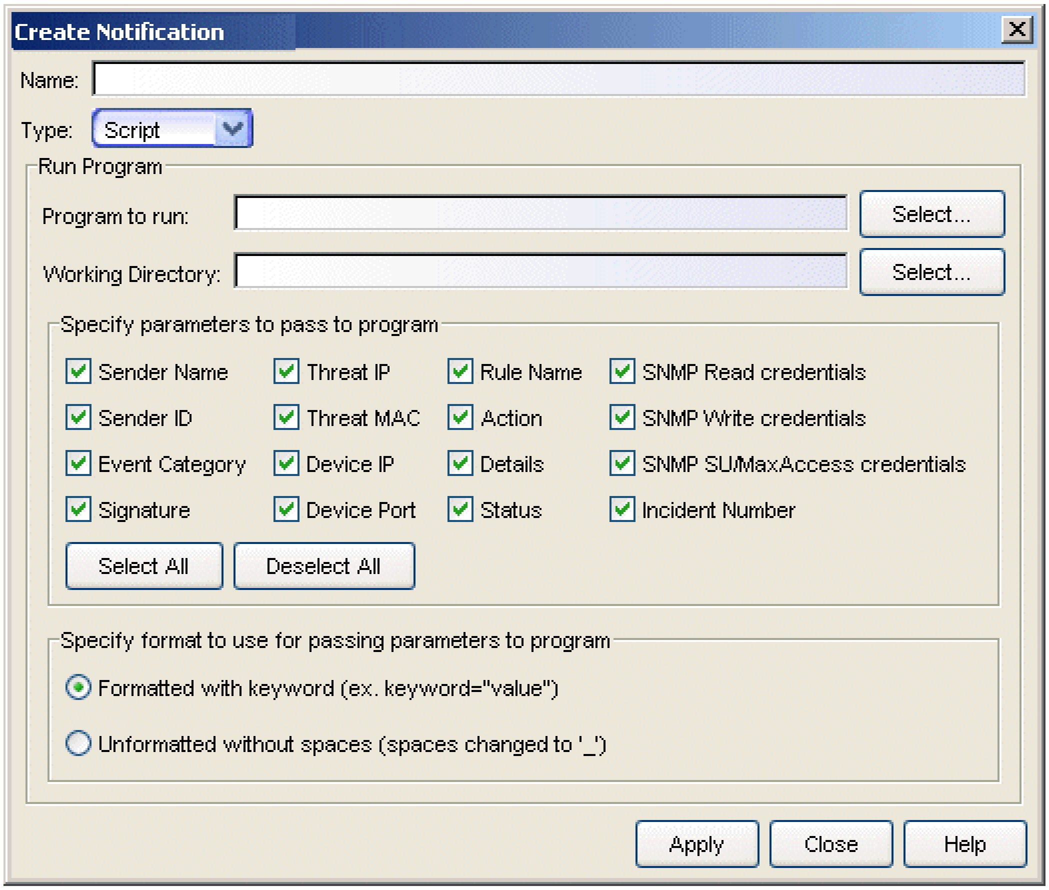
This is the password (between 1 and 64 characters in length) used to determine Privacy. This field is disabled if Privacy Type is **None**.

Trap Receiver

The IP address for a trap receiver (the system where devices send traps). Valid trap receivers are systems running a SNMPTrap Service.

Script

This window lets you identify a script executed with your response to network threats.



Create Notification

Name:

Type: Script

Run Program

Program to run:

Working Directory:

Specify parameters to pass to program

☑ Sender Name ☑ Threat IP ☑ Rule Name ☑ SNMP Read credentials

☑ Sender ID ☑ Threat MAC ☑ Action ☑ SNMP Write credentials

☑ Event Category ☑ Device IP ☑ Details ☑ SNMP SU/MaxAccess credentials

☑ Signature ☑ Device Port ☑ Status ☑ Incident Number

Specify format to use for passing parameters to program

● Formatted with keyword (ex. keyword="value")

○ Unformatted without spaces (spaces changed to '_')

Name

The name assigned to this notification.

Type

Set the Type to **Script** for this window.

Program to run

This field defines the script launched as this Custom Action. Scripts are stored in the <install directory>\NetSight\appdata\AutoSecMgr\scripts directory. Type a script name, if known, or use the **Select** button to open a file browser window and choose a script.

The **Program to run** field does not allow using options. For example, you cannot enter `myscript.bat -i <IP Address> -m <MAC Address>` in the Program to run field.

TIP: To execute a script with options, create a script without options that executes another script that has options (Windows only). For example:

1. Create a script named, `asm_script.bat` with an entry to call `myscript.bat` such as:

   C:\Program Files\My Custom Files\myscript.bat –i %1 -m %2".
2. Uncheck all but the **Threat IP** and **Threat MAC** checkboxes and select **Unformatted without spaces** (you don't want to send any keyword (thip= or thmac=) to your script.). The variable %1 returns <*Threat IP Address*> and %2 returns the <*Threat MAC Address*>

   If you are using PERL script, use a different argument variable, such as $ARGV[0] (First argument) or @ARGV (all arguments). Also, using the shell script is similar to a Windows batch file script (%1 for the first argument, %* for the all arguments).

Working Directory

This is the path to a directory from which the script executes. Any path references within your script that are not absolute paths, will be relative to this directory. Enter a path or use the Select button to open a file browser window and choose a directory.

Specify parameters to pass...

These check boxes let you select elements of the event information to be passed as parameters to your program. The Select All button places a check in all of the boxes and the Deselect All button removes checks from all of the boxes.

Specify format to use...

This area lets you select the format used to pass the selected parameters to your program:

Formatted with keyword...

When selected, passed parameters use a format that includes a keyword associated with each parameter (e.g., **`keyword="value"`**). So, for example, if Sender Name is selected as a parameter, the keyword sname is used and the information passed to the script is **`sname="dragon_id"`** followed by a space and then the keyword and value for the next parameter. The following table defines the keywords for each parameter and the order that the values are passed to the script (listed from top to bottom in the table).

Parameter	Keyword
Sender Name	sname
Sender ID	sid
Event Category	ecat
Signature	sig
Incident Number	incident
Threat IP	thip
Threat MAC	thmac
Device IP	dev
Device Port	port
Rule Name	rname
Action	action
Details	dtls
SNMP Parameters	see Note 1
Status	stat

Note 1: When selecting any SNMP parameter, **snmp=**_value_ indicates the SNMP version and the subsequent parameters contain the values assigned for the credentials associated with the device. When selecting multiple SNMP parameters (e.g., SNMP Write and SNMP Read) the values for the highest access level are used for the script.

SNMP v1, SNMPv2		SNMPv3	
Parameter	**Keyword**	**Parameter**	**Keyword**
SNMP Read	snmp="v1" ro	SNMP Read, SNMP Write, SNMP SU/Max Access	snmp="v3" user seclevel authtype authpwd privtype privpwd
SNMP Read	snmp="v1" rw		
SNMP Read	snmp="v1" su		

Example:

If you select Sender Name, Sender ID, Threat MAC, and SNMP Write and the device is configured for SNMPv1 credentials, the information passed to the script appears similar to the following:

```
sname="my sender name" sid="dragon id"
thmac="00.00.1d.11.22.33" snmp="v1" rw="public"
```

And, for a script named **myscript.bat**, the resulting script command is executed as:

```
C:\Program Files\Extreme
Networks\NetSight\appdata\AutoSecMgr\scripts\my_script.bat
sname="my sender name" sid="dragon id"
thmac="00.00.1d.11.22.33" snmp="v1" rw="public"
```

Unformatted without spaces...

When selected, the parameters are passed as space delimited, unformatted text, without keywords. For this option, your script must know which parameters are being passed and the order in which they are passed. If a parameter contains any spaces, they are replaced with an underscore (_).

Example:

You select Sender Name, Sender ID, Threat MAC, and SNMP Write and the device is configured for SNMPv1 credentials, the information passed to the script appears similar to the following:

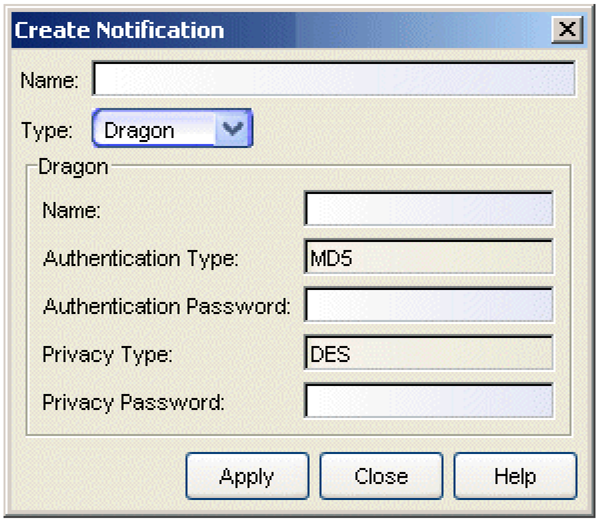
```
my_sender_name dragon_id 00.00.1d.11.22.33 v1 public
```

And, for a script named **myscript.bat**, the resulting script command is executed as:

```
C:\Program Files\Extreme
Networks\NetSight\appdata\AutoSecMgr\scripts\my_script.bat
my_sender_name dragon_id 00.00.1d.11.22.33 v1 public
```

Extreme Networks IPS

This window lets you configure a SNMPv3 trap notification sent to Extreme Networks Intrusion Prevention System (IPS) (formerly Dragon) when ASM responds to a network threat. This is similar to the SNMP Trap notification, except that for Extreme Networks IPS, you must specify an Authentication Type and Privacy Type.



Create Notification

Name:

Type: Dragon

Dragon

Name:

Authentication Type: MD5

Authentication Password:

Privacy Type: DES

Privacy Password:

Name

The name assigned to this notification.

Type

Set the Type to **Dragon** for this window.

Name

This is the user name for the credential used when sending the trap to the IPS.

Authentication Type

Select **MD5**, **SHA1**, or **None** from this drop-down menu.

Authentication Password

This is the password (between 1 and 64 characters in length) used to determine Authentication. This field is disabled if Authentication Type is **None**.

Privacy Type

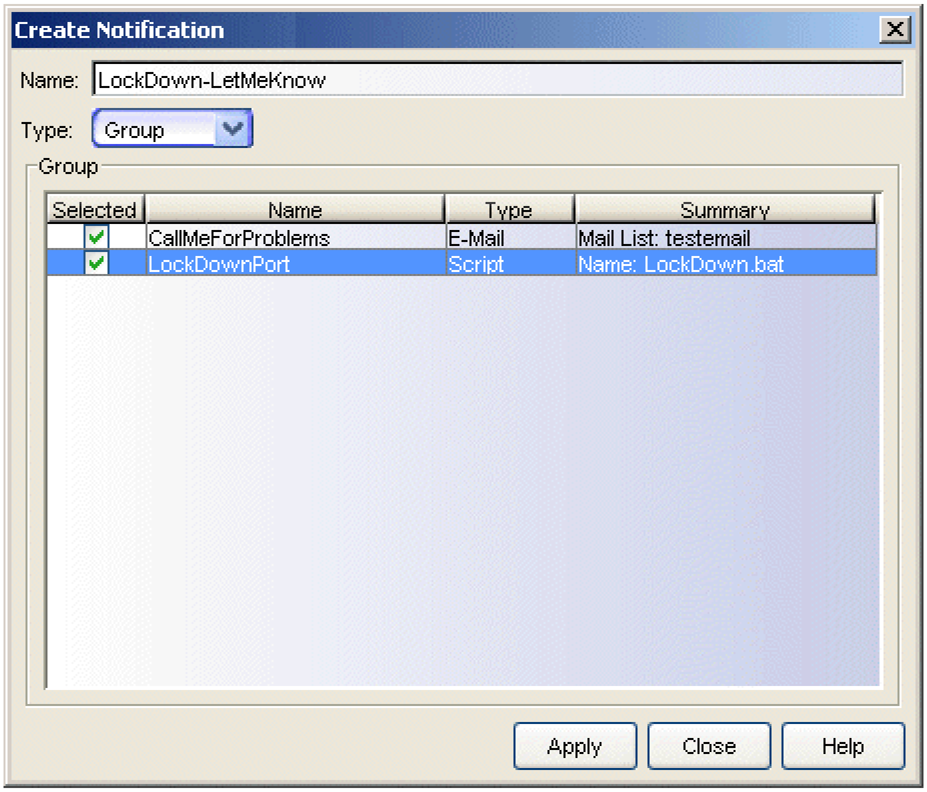
Select **DES** or **None** from this drop-down menu. These settings are disabled if Authentication Type is **None**.

Privacy Password

This is the password (between 1 and 64 characters in length) used to determine Privacy. This field is disabled if Privacy Type is **None**.

Group

This window lets you combine notifications in a group to provide multiple notifications when ASM responds to a network threat.



Create Notification

Name: LockDown-LetMeKnow

Type: Group

Group

Selected	Name	Type	Summary
☑	CallMeForProblems	E-Mail	Mail List: testemail
☑	LockDownPort	Script	Name: LockDown.bat

Name

The name assigned to this notification.

Type

Set the Type to **Group** for this window.

Group

This list shows all of the notifications (including other groups) included in this group. Checking selected groups and clicking **Apply** creates/edits the group with the checked notifications as members.

Related Information

For information on related windows:

- Error removing Notification(s) Window

For information on related tasks:

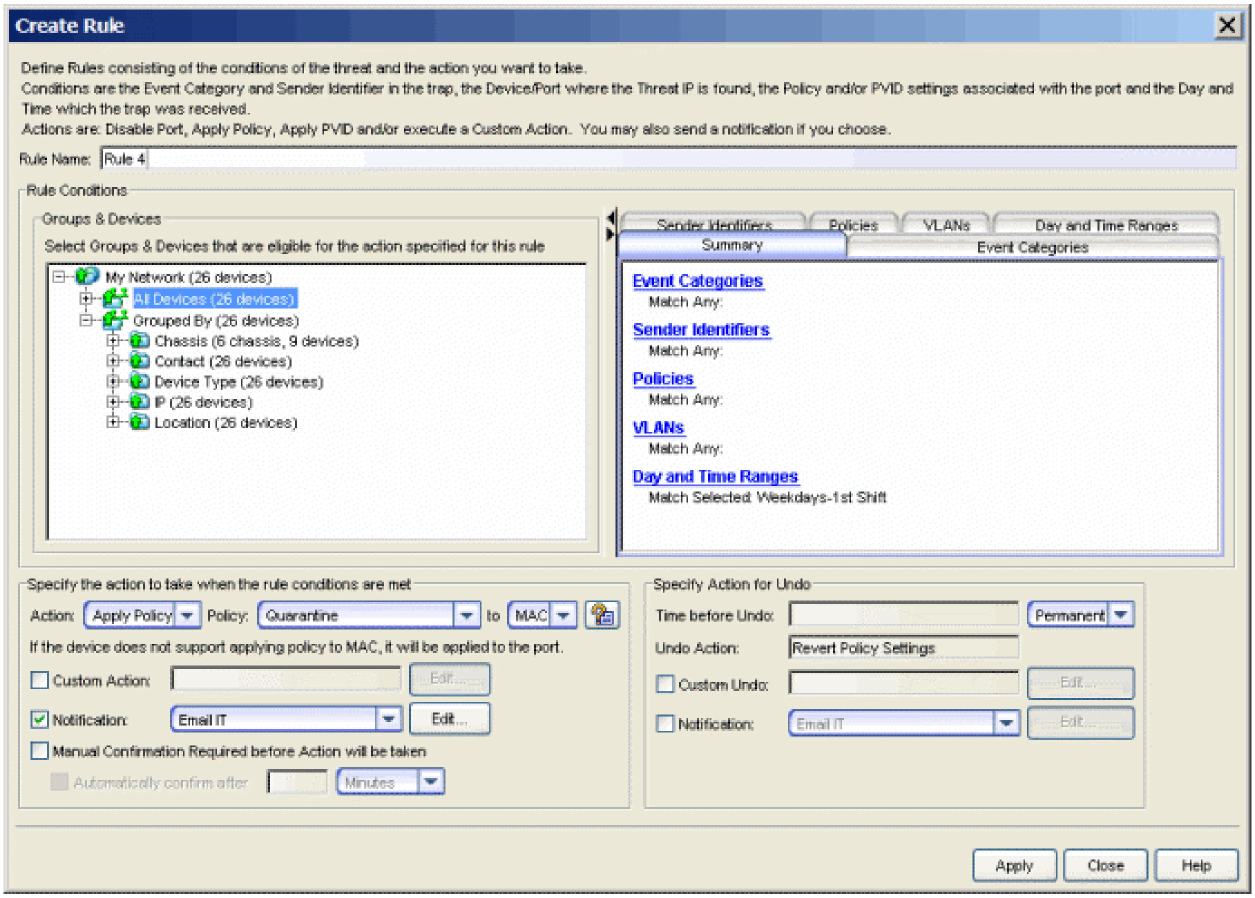
- How to Create and Edit Automated Security Manager Rules
- Using ASM Activity Monitor

Create/Edit Rule Window

The Create Rule and Edit Rule windows define new rules or modify existing rules used as Automated Security Manager responses to network security threats. The Edit Rule window opens with information for the rule selected in the Rule Definitions view, while the Create Rule window opens with blank or default settings.

Rules have two distinct functions:

- Examine the source of the threat (switch/port) to determine if certain conditions exist (e.g. threat category, source of the notifying IDS, policies currently applied to the port, etc.).
- Define the action taken when these conditions match the criteria defined by the Rule.



Create Rule

Define Rules consisting of the conditions of the threat and the action you want to take.
Conditions are the Event Category and Sender Identifier in the trap, the Device/Port where the Threat IP is found, the Policy and/or PVID settings associated with the port and the Day and Time which the trap was received.
Actions are: Disable Port, Apply Policy, Apply PVID and/or execute a Custom Action. You may also send a notification if you choose.

Rule Name: Rule 4

Rule Conditions

Groups & Devices

Select Groups & Devices that are eligible for the action specified for this rule

My Network (26 devices)
All Devices (26 devices)
Grouped By (26 devices)
Chassis (6 chassis, 9 devices)
Contact (26 devices)
Device Type (26 devices)
IP (26 devices)
Location (26 devices)

Event Categories
Match Any:
Sender Identifiers
Match Any:
Policies
Match Any:
VLANs
Match Any:
Day and Time Ranges
Match Selected: Weekdays-1st Shift

Specify the action to take when the rule conditions are met

Action: Apply Policy Policy: Quarantine to MAC

If the device does not support applying policy to MAC, it will be applied to the port.

☐ Custom Action:

☑ Notification: Email IT

☐ Manual Confirmation Required before Action will be taken

☐ Automatically confirm after Minutes

Specify Action for Undo

Time before Undo: Permanent

Undo Action: Revert Policy Settings

☐ Custom Undo:

☐ Notification: Email IT

Name

The name given to this rule. The name can be any character string, excluding spaces, up to 64 characters.

Rule Conditions

The following attributes are compared against the device(s) located by the ASM search and the event information reported by the IDS to determine the applicability of the specified action. When the information from the search and the event information match these attributes, then the action specified below is applied.

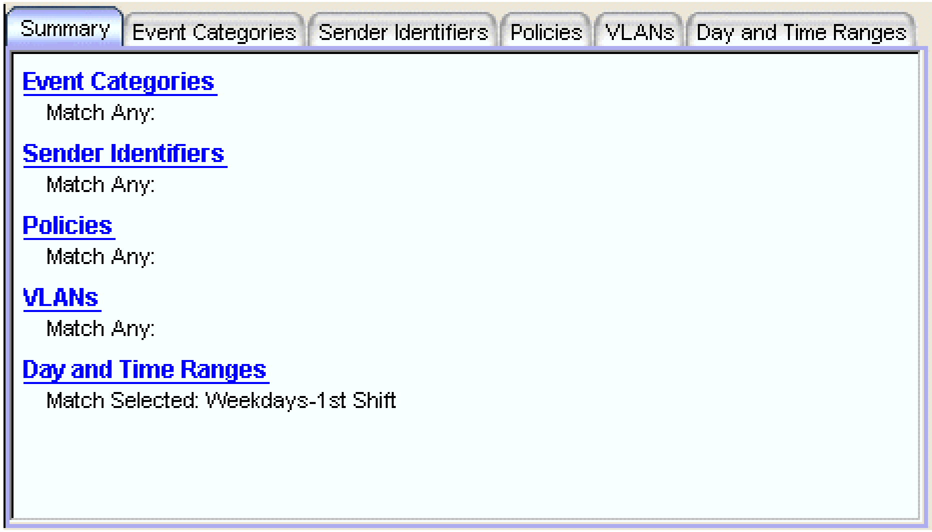
Groups & Devices

The tree in this panel can be expanded to select a target device or device group that is eligible for the action specified in the rule. You can create several rules to respond to a particular threat and apply different actions based on the device/device group selected here. For example, if you are creating a rule with an action that applies a policy, you do not want to select a device/device group for a device type that does not support policies. Or as another example, in some rules, you may want to apply different actions or more or less permanent actions for certain subnets containing critical network resources.

NOTE: Do not select the Layer 3 NAC Controller and the NAC Gateway appliance as a device eligible for the action specified in the rule.

Qualifier Tabs

Summary



Event Categories
Match Any:

Sender Identifiers
Match Any:

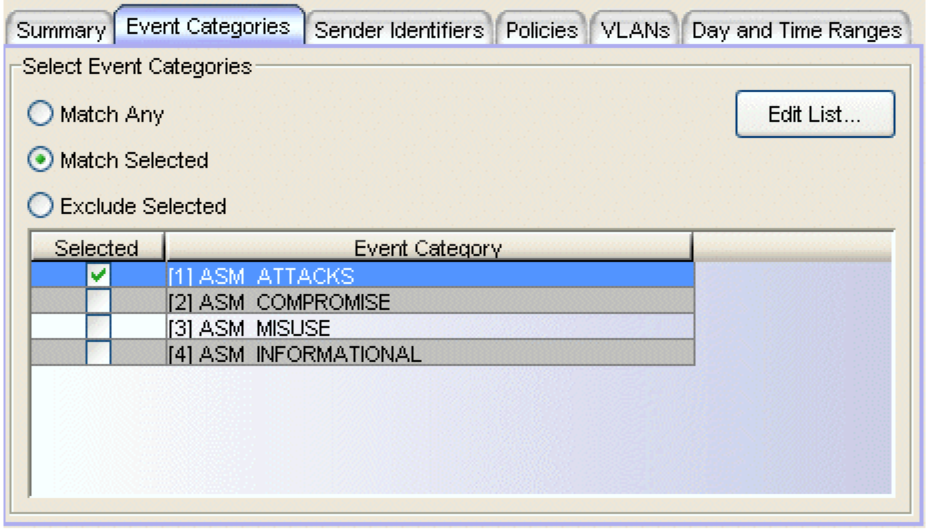
Policies
Match Any:

VLANs
Match Any:

Day and Time Ranges
Match Selected: Weekdays-1st Shift

This tab shows a summary of the currently defined qualifiers for this rule. Clicking a particular heading selects that tab.

Event Categories



Select Event Categories

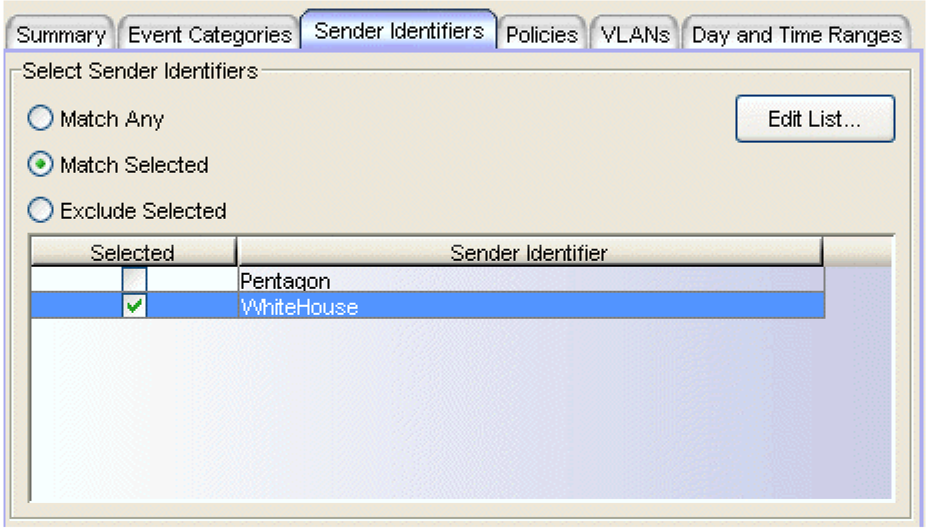
○ Match Any
● Match Selected
○ Exclude Selected

Selected	Event Category
☑	[1] ASM_ATTACKS
□	[2] ASM_COMPROMISE
□	[3] ASM_MISUSE
□	[4] ASM_INFORMATIONAL

This tab lets you select one or more event categories, reported by the IDS, to determine whether or not to apply an action.

- **Match Any** - This is an unconditional match for the category.
- **Match Selected** - The event category is compared against one or more categories selected from the list.
- **Exclude Selected** - The event category matches if it is not one of the categories selected from the list.

Sender Identifiers



Select Sender Identifiers

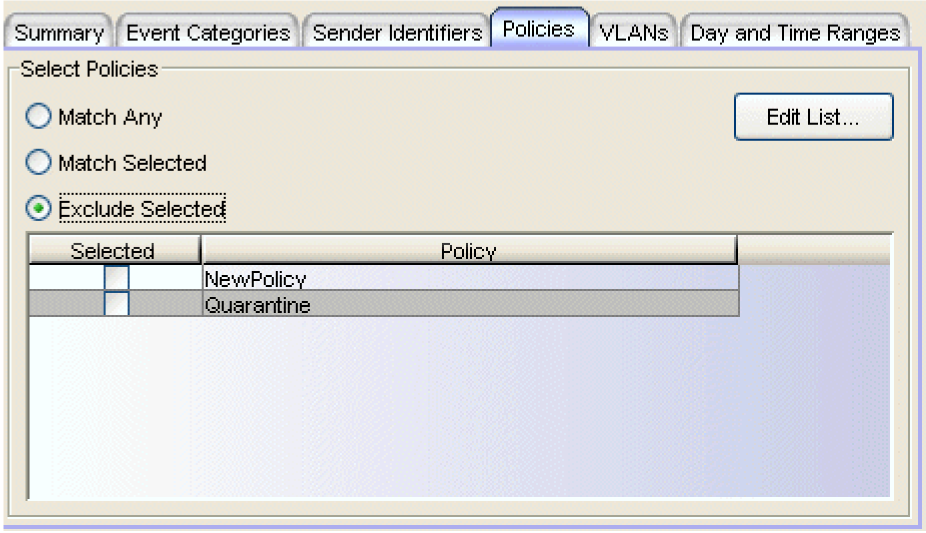
○ Match Any
● Match Selected
○ Exclude Selected

Selected	Sender Identifier
□	Pentagon
☑	WhiteHouse

This tab lets you select one or more unique identifiers, associated with the intrusion detection systems that detected the security event, to determine whether or not to apply an action.

- **Match Any** - This is an unconditional match for the Sender ID.
- **Match Selected** - The Sender ID is compared against one or more Sender Identifiers selected from the list.
- **Exclude Selected** - The Sender ID matches if it is not one of the Sender Identifiers selected from the list.

Policies



Select Policies

○ Match Any

○ Match Selected

● Exclude Selected

Selected	Policy
□	NewPolicy
□	Quarantine

This tab lets you select one or more policies to determine whether or not to apply an action.

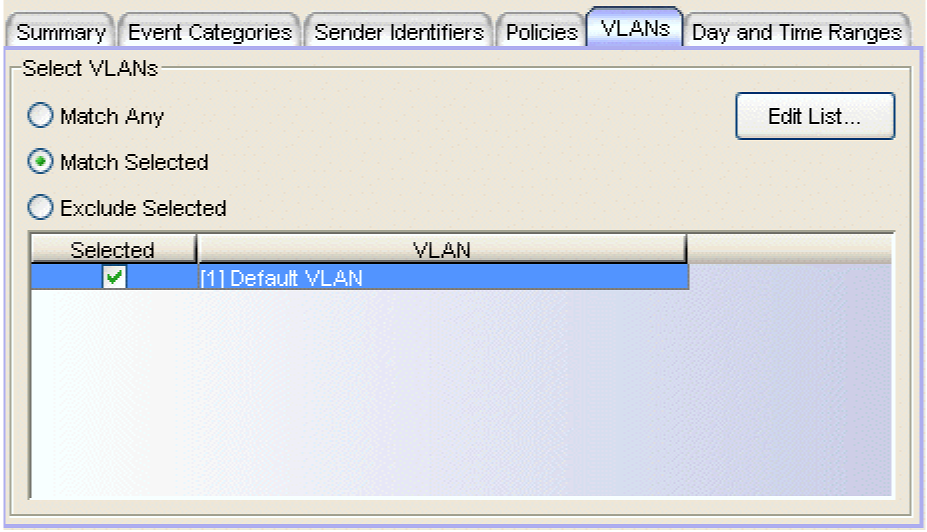
- **Match Any** - This is an unconditional match for a currently applied policy.
- **Match Selected** - A match occurs when the currently applied policy is one of policies selected in the list.
- **Exclude Selected** - A match occurs when the currently applied policy is not one of the policies selected in the list.

IMPORTANT:
Whether or not a policy matches a selection from the Policy List depends on the operational mode/features supported on specific device types:

- N-Series Platinum:
  - Multi-auth - The Apply Policy action determines the specific policy being matched. If the action is **Apply Policy** to **Port**, then only port policies are compared to your selection(s) from the Policy List.
  - StrictX - Same as N-Series Platinum in multi-auth mode, except the port-based policy is used for authentication. In any case, the policy matching works the same way as the N-Series Platinum (multi-auth).

- N-Series Gold:
    - Multi-auth - N-Series Gold does not support MAC/IP override. As a result, the only ASM action you can take for applying a policy is to **Apply Policy** to **Port**. Policy matching always compares the policy(ies) selected in the Policy List against the policy currently in effect.
- C2: Functions the same way as the N-Series Gold (StrictX).
- E1/E7: Policy matching always compares the policies selected from the Policy List against the policy currently in effect on the port.

VLANs



Select VLANs

○ Match Any

● Match Selected

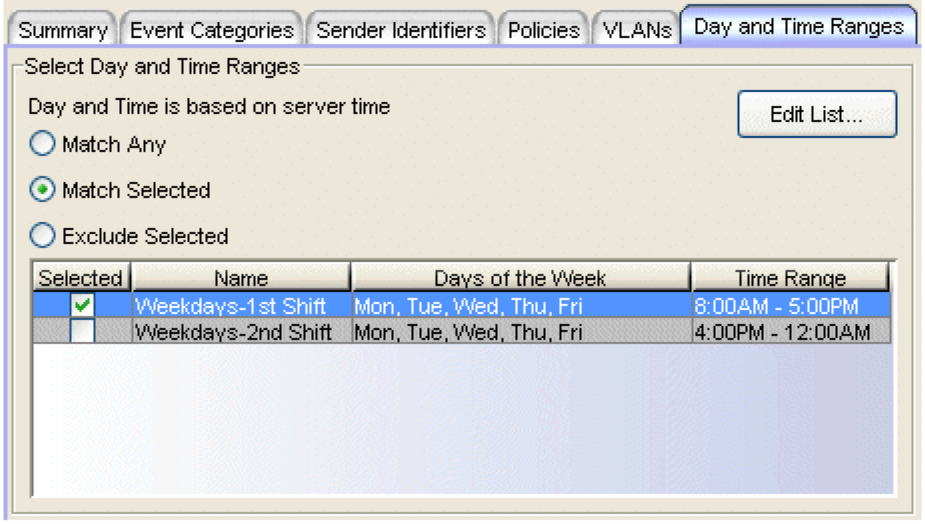
○ Exclude Selected

Selected	VLAN
☑	[1] Default VLAN

This tab lets you select one or more VLANs, currently applied on the port, to determine whether or not to apply an action.

- **Match Any** - This is an unconditional match for a currently applied VLAN.
- **Match Selected** - The currently applied VLAN is compared against one or more VLANs selected from the list.
- **Exclude Selected** - The currently applied VLAN is not one of the VLANs selected from the list.

Day and Time Ranges



Select Day and Time Ranges

Day and Time is based on server time

○ Match Any

● Match Selected

○ Exclude Selected

Selected	Name	Days of the Week	Time Range
☑	Weekdays-1st Shift	Mon, Tue, Wed, Thu, Fri	8:00AM - 5:00PM
□	Weekdays-2nd Shift	Mon, Tue, Wed, Thu, Fri	4:00PM - 12:00AM

This tab lets you select one or more of your previously defined intervals, covering specific days and times, to determine whether or not to apply an action.

Specify the action to take...

This area defines the actions to be taken when the event matches the above criteria set by a rule. It allows taking a specific action on a port, MAC address, or IP address or taking a Custom Action (launching a program to be run).

Action

Use this drop-down menu to select a response to the threat: **None**, **Disable Port**, **Apply Policy**, **Apply PVID, or Notify NAC**.

Apply Policy

Use the Policy drop-down menu to select a policy to be applied on the device. The available policies are listed in the **Policies** tab. You must also specify whether to apply the policy to the MAC source, IP source, or the port.

Multi-User Authentication

When the action for a rule is set to **Apply Policy** and the threat is located on a port on a device that supports Multi-User Authentication (e.g., Matrix DFE), you can apply a policy to a specific MAC address or IP address. This lets you isolate a single user instead of affecting all of the users on the port. You can apply a user-specific policy to an IP address or MAC address instead of changing the port policy. If the threat MAC address is unique to a particular Threat IP (typically on devices at the edge of your network), select **MAC** to apply the policy to the MAC address and override its port or dynamic policy. If the threat is on a device at the core of your network and the MAC address maps to several IP addresses, select **IP** to apply the policy to the IP address and override its port or dynamic policy.

NOTE: Policies applied to a MAC source override policies applied to an IP source. So, if there is a policy currently applied to a MAC source, applying a policy to an IP-source policy has no effect. See also the IMPORTANT Policy Matching notes, above.

Apply PVID

Use the PVID drop-down menu to select the PVID applied to the port. The available VLANs are defined in the Automated Security Manager Rule Variables - VLANs view. The associated **PVID Egress** drop-down menu lets you either retain the current PVID egress state by selecting **None** or change the egress state to **Untagged**. When **Untagged** is selected, the PVID is applied and the egress state is set to **Untagged**. When **None** is selected, the egress state is unchanged and only the PVID is applied. If you have specified a Discard VLAN as the PVID, selecting **None** usually means traffic is discarded.

NOTE: Applying a PVID to a port does not clear the VLAN from egress lists for non-PVID VLANs. This is normal operation. If *Apply PVID* is selected, change the egress state to ***Untagged*** or apply a quarantine policy to the port.

Notify NAC

When **Notify NAC** is selected, ASM notifies NAC Manager in response to a real-time security threat from an end-system on the network. NAC Manager automatically adds the end-system's MAC address to the Blacklist end-system group, effectively putting the end-system in quarantine and preventing the end-system from accessing the network from any location. If ASM notifies NAC Manager the security threat is no longer present, then NAC Manager removes the end-system from the Blacklist group and the end-system is dynamically re-authenticated to the network. You can view ASM blacklists in the NAC Manager Advanced Configuration view, by selecting **Tools > Manage Advanced Configurations** from the menu bar. In the left-panel tree, expand the Rule Components folder and the End-System

Group folder, and click on Blacklist. An ASM blacklist entry has a description of "ASM."

Custom Action

Check **Custom Action** and click **Edit** to open the Specify Program for Action window where you can customize the response to an event by selecting a program to execute.

> **NOTE:** When a custom action script does not specify the path for its output, the output is placed in the `<install directory>\NetSight\jboss\bin directory`.

Notification

You can specify a notification to be part of the rule's action. For example, you can specify that an E-Mail notification is sent in response to a threat. Check **Notification** and select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window, which lists the configured notifications. In this window, you can select a Notification to edit, or click **Create** to open the Create Notification window.

> **NOTE:** If you create a rule with an action that requires a manual confirmation, and an email notification is configured for the action, you can use the Advanced Settings option (Tools > Options) so ASM also sends an email notification when the action needs to be confirmed. The notification has a subject line of "Awaiting Manual Confirmation." Once the action is performed, the notification is sent again, with the subject line originally defined in the notification.

Manual Confirmation Required

When checked, the selected action requires human intervention before executing. The action/event must be selected in the Automated Security Manager Activity Monitor and confirmed with the **Confirm Response** button.

Automatically confirm after

When checked, the selected action is automatically confirmed if not manually confirmed prior to the specified time.

Specify Action for Undo

With one exception, you can undo applied actions. The exception can occur when two actions are defined within a rule: a standard ASM action and a custom action. If the standard ASM action fails, the custom action applies and, if successful, cannot be undone. Under these circumstances, configure your custom action to take into account the potential failure of the standard ASM action.

Time before Undo

This setting determines whether the action is **Permanent** or set to a time span of **Minutes**, **Hours** as defined in the associated field. **Permanent** means that ASM does not automatically undo the action after a certain time interval, but it can still be manually undone.

Undo Action

This field shows an Undo Action that corresponds to the **Action** previously selected/applied to a port. It cannot be edited.

Custom Undo

Check **Custom Undo** and click **Edit** if you want to specify an action taken when an action is undone. This opens the Specify Program for Undo window where you can select a program to be executed. This does not alter the Undo Action, the Custom Undo is executed in addition to the Undo Action.

NOTE: When a custom undo action script does not specify the path for its output, the output is placed in the `<install directory>\NetSight\jboss\bin` directory.

Notification

You can specify a notification to be part of the rule's action. For example, you can specify an E-Mail notification to be sent in response to a threat. Check **Notification** and select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window which lists the configured notifications. In this window, you can select a Notification to edit, or click **Create** to open the Create Notification window.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- ASM Activity Monitor

For information on related tasks:

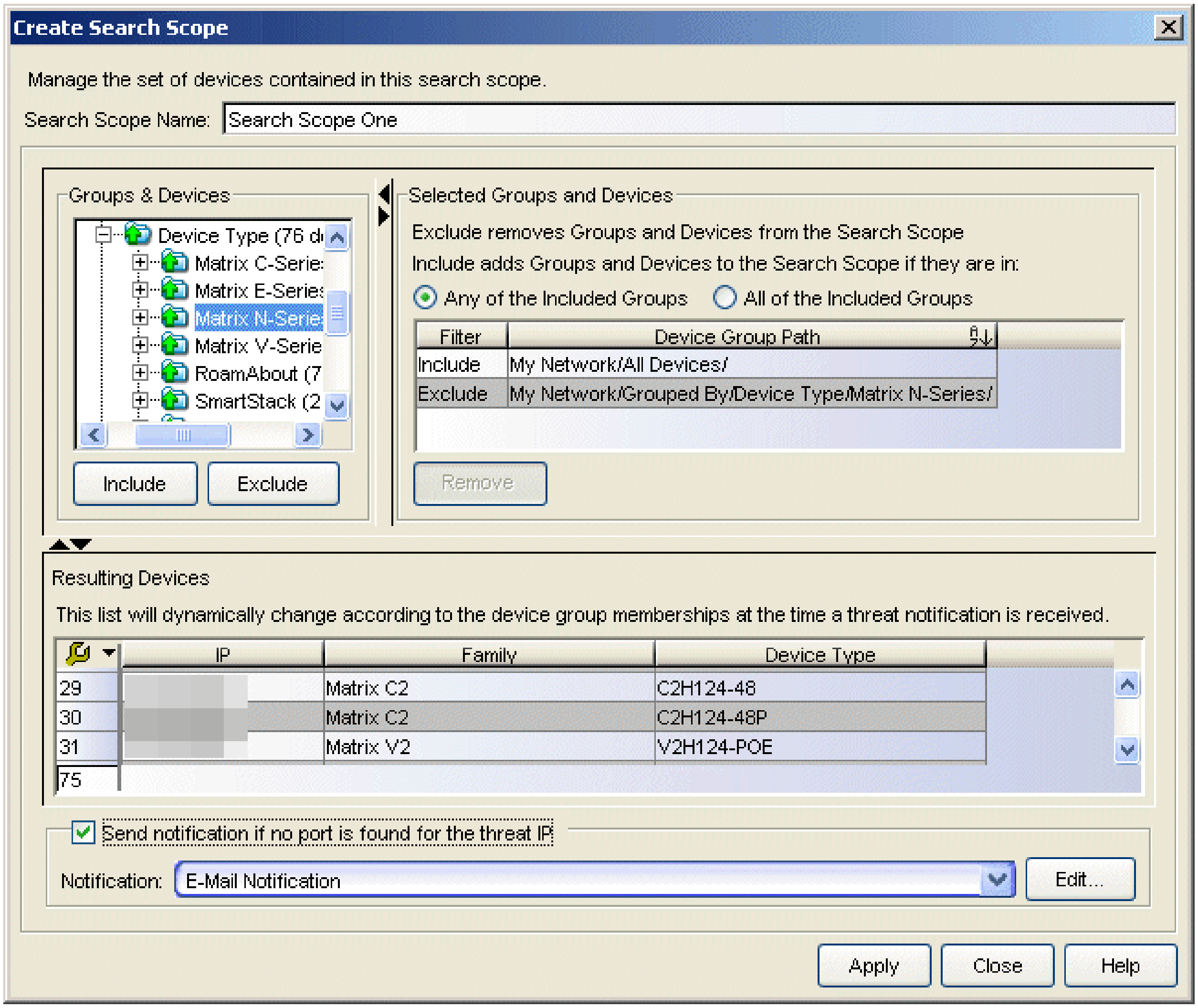
- How to Create and Edit Rules
- How to Use ASM Activity Monitor

Create/Edit Search Scope Window

This window lets you create and name groups of devices searched when Extreme Networks IPS notifies ASM of a threat. It operates the same way as the settings for the Basic Search Scope Definitions, but allows you to create multiple search scope groups so you can search several non-contiguous groups of devices. You can include or exclude specific devices, according to Device Type, Location, Contact, and Subnet.

You can access this window from the ASM Configuration window's Search Scope Definitions panel. Select the Advanced Search Mode, then click the **Create** or **Edit** button in the Search Scopes section.

NOTE: The NetSight Server performs ASM searches using the profile for the server, not the profile for the ASM client user.



Manage the set of devices contained in this search scope.

Search Scope Name: Search Scope One

Selected Groups and Devices

Exclude removes Groups and Devices from the Search Scope

Include adds Groups and Devices to the Search Scope if they are in:

● Any of the Included Groups ○ All of the Included Groups

Filter	Device Group Path
Include	My Network/All Devices/
Exclude	My Network/Grouped By/Device Type/Matrix N-Series/

Resulting Devices

This list will dynamically change according to the device group memberships at the time a threat notification is received.

	IP	Family	Device Type
29	[redacted]	Matrix C2	C2H124-48
30	[redacted]	Matrix C2	C2H124-48P
31	[redacted]	Matrix V2	V2H124-POE
75			

☑ Send notification if no port is found for the threat IP

Notification: E-Mail Notification

Search Scope Name

The name given to this search scope. The name can be any character string, up to 64 characters.

Groups & Devices

This panel shows the device tree for devices modeled in the Console database. You can expand branches of the tree to select the Devices/Device Groups to search when Extreme Networks IPS notifies ASM of a threat. After making a selection, click **Include** to designate your selection(s) as being included in the search scope or click **Exclude** to designate your selection(s) as being specifically excluded in the search scope.

You can repeatedly select devices/device groups individually and click Include/Exclude or use multiple selection techniques (Control-click or Shift-Click) to select or de-select multiple Devices/Device Groups in a single operation.

NOTES: 1. When there are devices on your network that do not support layer 3, include routers in the list of targets to allow Compass to use its IP to MAC address resolution feature to locate the end station. This includes the following devices: C1, E1 (1G6xx Series), E5, V-Series, SS9000, Vertical Horizon, 1st Generation 1Hxxx Series.

Do **not** use the Layer 3 NAC Controller and the NAC Gateway as a search device in ASM. Configure ASM to search other devices in the network for the IP-to-MAC-to-port bindings, such as gateway routers for IP-to-MAC bindings and access edge switches for MAC-to-port information.

Selected Groups and Devices

This panel lists the devices/device groups selected from the Groups & Devices panel. The **Filter** column in the table indicates whether the device (s)/device group(s) can be included or excluded. The **Device Group Path** column shows the specific IP address and branch of the tree for selected devices/device groups.

Devices/device groups designated as Excluded are excluded from the search scope, regardless of any Include settings. For example, if a particular device is set to Excluded and the same device is a member of a device group that is set to Included, then the excluded device is not searched.

You can further refine your search scope by selecting either **Any of the Included Groups** or **All of the Included Groups**.

- **Any of the Included Groups** creates an OR condition so if a selected device (not specifically excluded) is a member of any of the selected groups, then it is included in the search scope and appears in the Resulting Device/Device Group table. For example, selecting a specific Vertical Horizon device not in subnet 172.18.19.xx together with the *Vertical Horizon* and *IP Subnet 172.18,19.xx* Device Groups and clicking **Any of the Included Groups** includes all Vertical Horizon devices (including the individual VH device) and all devices from the 172.18,19.xx subnet.
- **All of the Included Groups** creates an AND condition. When selected, only devices that are members of all of the selected device groups are included in the search scope. This selection is useful when you want to

select all of a particular device type, but only in a specific location--for example, all the routers in a particular building. When a device type (Routers) and a location group (Building2) are both selected, then only the devices contained in both groups (Routers in Building2) are included in the search scope.

Resulting Devices

The resulting list of devices searched when Extreme Networks IPS notifies ASM of a threat. The table is dynamically updated according to your device/device group selections and include/exclude arguments.

Send Notification...

This checkbox allows you to select a notification to be performed in the event no port is found for the Threat IP. For example, you can specify an E-Mail notification to be sent when no port is found. Select the desired notification from the drop-down menu. Click **Edit** to open the Edit Notifications window, which lists the configured notifications. In this window, you can select a notification to edit, or click **Create** to open the Create Notification window.

Include/Exclude

Adds your tree selections to the Selected Groups and Devices table and sets the Filter column to either Include or Exclude.

Remove

Deletes one or more rows selected from the **Groups and Devices** table.

Apply

Creates the search scope group and adds it to the **Search Scopes** table in the Advanced Search Scope Definition view of the Automated Security Manager Configuration Window.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Automated Security Manager Activity Monitor

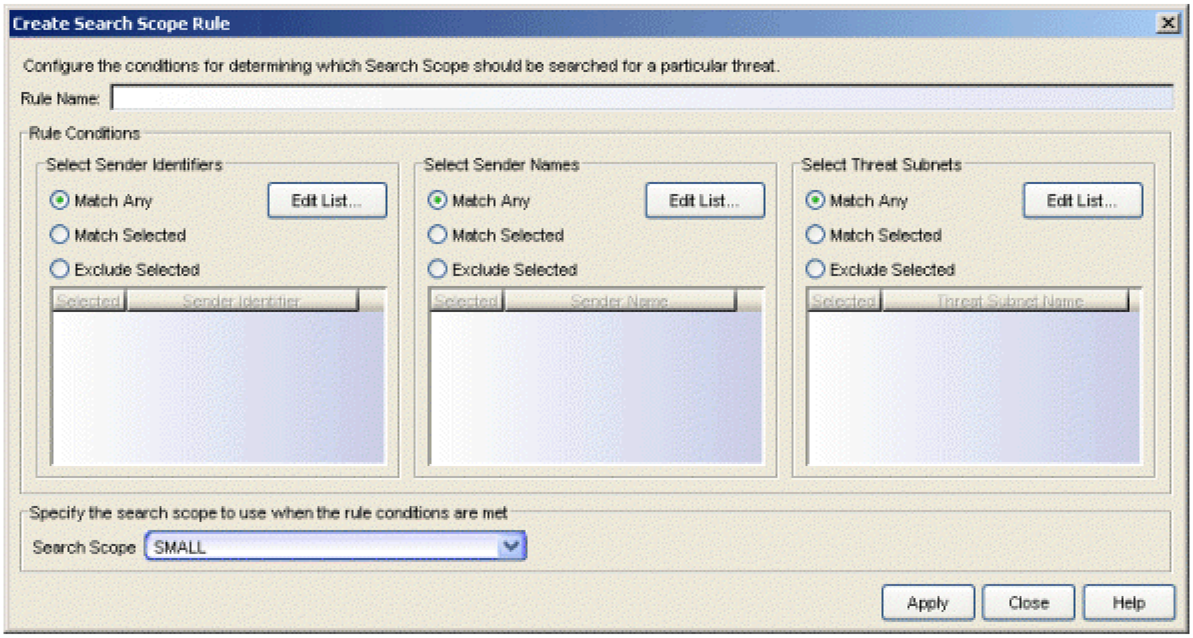
For information on related tasks:

- How to Set Automated Security Manager Options
- How to Create and Edit Automated Security Manager Rules
- How to Use Automated Security Manager Activity Monitor

Create/Edit Search Scope Rule Window

This window lets you create rules that determine which search scope is used when a specific threat arrives. Each search scope rule contains a set of conditions (sender id, threat subnet, etc.) and defines the search scope to use when the conditions are met.

You can access this window from the ASM Configuration window's Search Scope Definitions panel. Select the Advanced Search Mode, then click the Create or Edit button in the Search Scope Rules section.



Create Search Scope Rule

Configure the conditions for determining which Search Scope should be searched for a particular threat.

Rule Name:

Rule Conditions

Select Sender Identifiers
- ● Match Any
- ○ Match Selected
- ○ Exclude Selected

Selected	Sender Identifier

Select Sender Names
- ● Match Any
- ○ Match Selected
- ○ Exclude Selected

Selected	Sender Name

Select Threat Subnets
- ● Match Any
- ○ Match Selected
- ○ Exclude Selected

Selected	Threat Subnet Name

Specify the search scope to use when the rule conditions are met

Search Scope: SMALL

Rule Name

The name given to this rule. The name can be any character string, up to 64 characters.

Rule Conditions

The following conditions are compared against the information returned from Extreme Networks IPS to determine the applicability of this rule. When the information from the event information matches these conditions, then the Search Scope specified is used as the ASM search scope.

Select Sender Identifiers

This area lets you select one or more sender identifiers to be compared against the sender identifier returned in the event, which determines whether or not to use the Search Scope specified as the ASM search scope.

- Match Any - This is an unconditional match for the Sender ID.
- Match Selected - The Sender ID is compared against one or more Sender Identifiers selected from the list.
- Exclude Selected - The Sender ID matches if it is not one of the Sender Identifiers selected from the list.

Use the Edit List button to open a window where you can add or remove sender identifiers to use in your rule definitions.

Select Sender Names

This area lets you select one or more sender names to be compared against the sender name returned in the event, which determines whether or not to use the Search Scope specified as the ASM search scope.

- Match Any - This is an unconditional match for the Sender Name.
- Match Selected - The Sender Name is compared against one or more Sender Names selected from the list.
- Exclude Selected - The Sender Name matches if it is not one of the Sender Names selected from the list.

Use the Edit List button to open a window where you can add or remove sender names to use in your rule definitions.

Select Threat Subnets

This area lets you select one or more subnets to be compared against the subnet returned in the event, which determines whether or not to use the Search Scope specified as the ASM search scope.

- Match Any - This is an unconditional match for the Threat Subnet.
- Match Selected - The Threat Subnet is compared against one or more Threat Subnets selected from the list.
- Exclude Selected - The Threat Subnet matches if it is not one of the Threat Subnets selected from the list.

Use the Edit List button to open a window where you can add or remove threat subnets to use in your rule definitions.

Search Scope

This drop-down menu lets you select a Search Scope Group used as the ASM search scope when an event matches the conditions defined for this rule.

Related Information

For information on related windows:

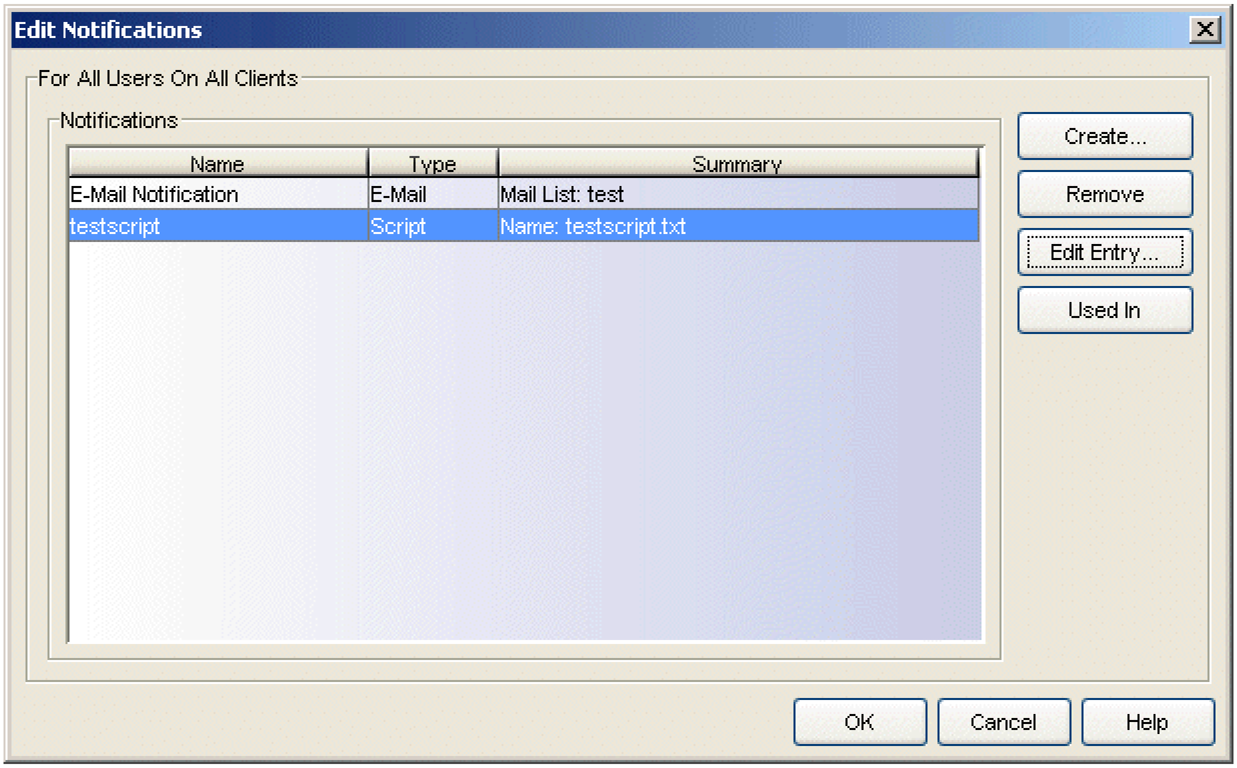
- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Automated Security Manager Activity Monitor

For information on related tasks:

- How to Set Automated Security Manager Options
- How to Create and Edit Automated Security Manager Rules
- How to Use Automated Security Manager Activity Monitor

Edit Notifications Window

This window lists all the notifications you have created, and lets you edit or remove a notification, or create a new one.



Name	Type	Summary
E-Mail Notification	E-Mail	Mail List: test
testscript	Script	Name: testscript.txt

Name

The name assigned to this notification in the Create/Edit Notification window.

Type

The type of notification, as selected in the Create/Edit Notification window.

Summary

The variables configured for this notification in the Create/Edit Notification window.

Create

Opens the Create Notification window. This window takes one of several forms, depending on the type of notification being created (E-Mail, Syslog, SNMP Trap, Script, Dragon, or Group).

Remove

Removes the selected notifications from the list. You cannot remove notifications if they are currently in use by a rule. Attempting to remove a notification currently in use by a rule opens the Error removing Notification (s) window to show the rules where the selected notifications are used.

Edit Entry

Opens the Edit Notification window for the notification selected in the list.

Used In

Select a notification in the list, and click the **Used In** button to open a window that displays which ASM rules are using the notification.

Related Information

For information on related windows:

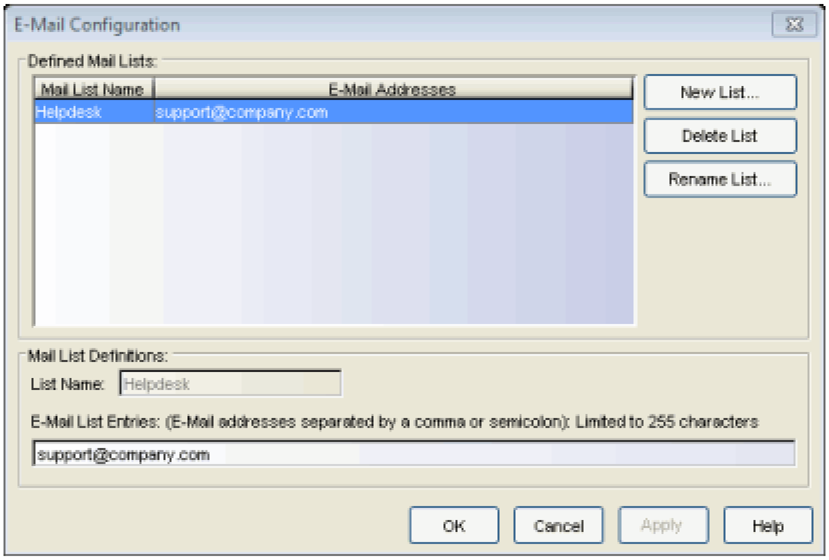
- ASM Configuration Window
- Create/Edit Rule Window

For information on related tasks:

- How to Create and Edit Automated Security Manager Rules
- Using the Automated Security Manager Activity Monitor

E-Mail Configuration Window

The E-Mail Configuration window lets you create an e-mail recipient list to use when configuring e-mail notification settings. The window is accessed from the Edit Mail List button in the Create/Edit Notification window.



Mail List Name	E-Mail Addresses
Helpdesk	support@company.com

List Name: Helpdesk

E-Mail List Entries: (E-Mail addresses separated by a comma or semicolon): Limited to 255 characters

support@company.com

Defined Mail Lists

Displays the currently defined mail lists. Use the **New List** button to add a mail list name to the list.

Mail List Definitions

Use the E-Mail List Entries field to configure the "send to" e-mail addresses for the selected list. Addresses in the list can be separated with a comma or a semicolon. The list is not verified for valid addresses.

New List

Lets you create a new mail list name.

Delete List

Deletes the selected list.

Rename List

Lets you rename the selected list.

Related Information

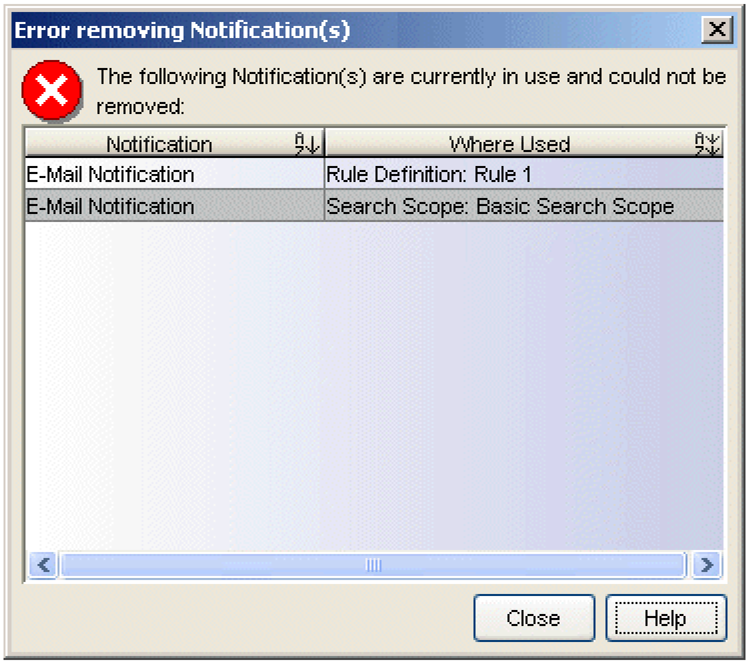
For information on related windows:

- Create/Edit Notification Window
- Create/Edit Rule Window

Error removing Notification(s) Window

This window automatically opens if you attempt to remove one or more notifications currently in use by ASM. The table lists the specific notification(s) causing the error and indicates where each notification is being used.

Sample Error removing Notification(s) Window



The following Notification(s) are currently in use and could not be removed:

Notification	Where Used
E-Mail Notification	Rule Definition: Rule 1
E-Mail Notification	Search Scope: Basic Search Scope

Related Information

For information on related windows:

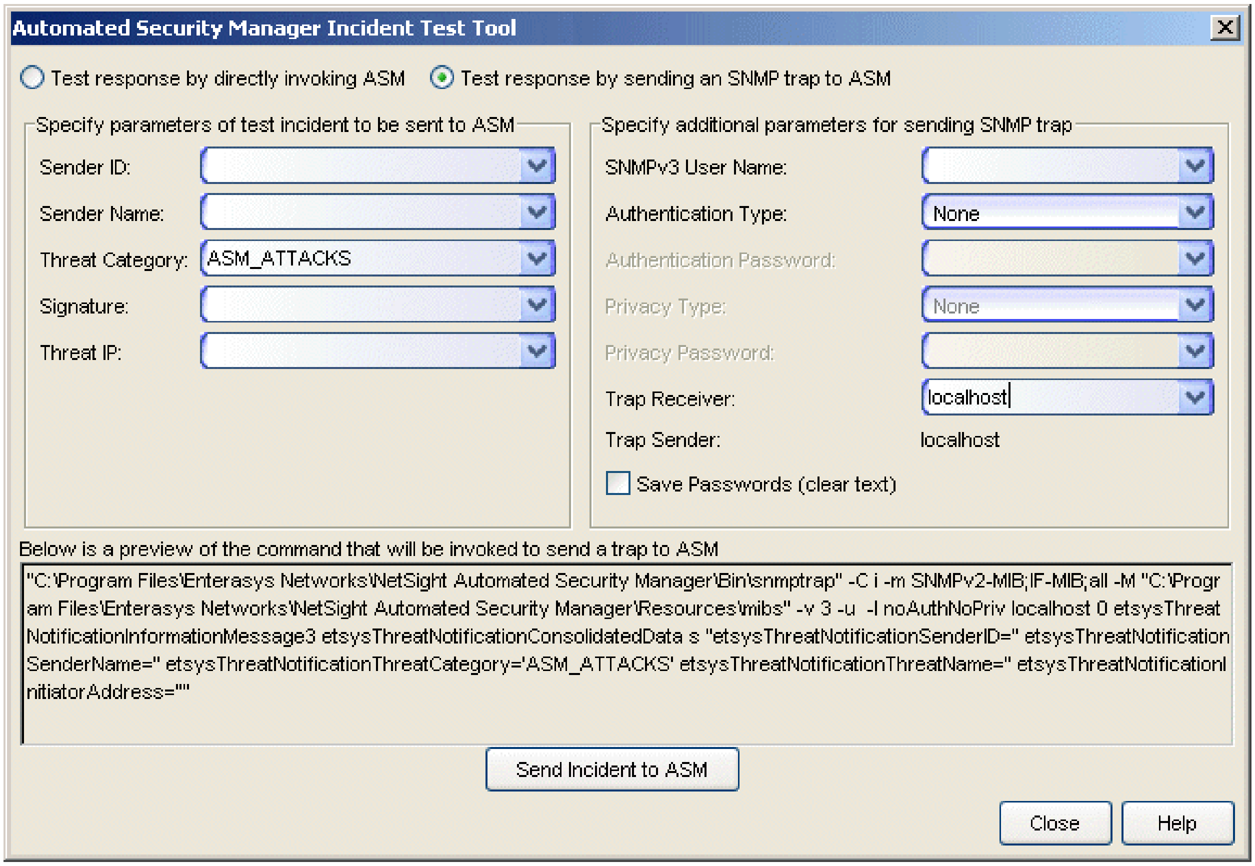
- Create/Edit Notification Window

For information on related tasks:

- How to Create and Edit Automated Security Manager Rules
- Using the Automated Security Manager Activity Monitor

Incident Test Tool

This tool lets you test and debug the search scopes and actions to verify ASM's response to an event.



○ Test response by directly invoking ASM ● Test response by sending an SNMP trap to ASM

Specify parameters of test incident to be sent to ASM

Sender ID:

Sender Name:

Threat Category: ASM_ATTACKS

Signature:

Threat IP:

Specify additional parameters for sending SNMP trap

SNMPv3 User Name:

Authentication Type: None

Authentication Password:

Privacy Type: None

Privacy Password:

Trap Receiver: localhost

Trap Sender: localhost

□ Save Passwords (clear text)

Below is a preview of the command that will be invoked to send a trap to ASM

```
"C:\Program Files\Enterasys Networks\NetSight Automated Security Manager\Bin\snmptrap" -C i -m SNMPv2-MIB;IF-MIB;all -M "C:\Progr
am Files\Enterasys Networks\NetSight Automated Security Manager\Resources\mibs" -v 3 -u  -l noAuthNoPriv localhost 0 etsysThreat
NotificationInformationMessage3 etsysThreatNotificationConsolidatedData s "etsysThreatNotificationSenderID='' etsysThreatNotification
SenderName='' etsysThreatNotificationThreatCategory='ASM_ATTACKS' etsysThreatNotificationThreatName='' etsysThreatNotificationI
nitiatorAddress=''"
```

Two levels of testing can be performed:

- **Test response by sending an SNMP trap to ASM** - This level uses Console's SNMPTrap Service to receive the trap and notify ASM of the threat. This is the more comprehensive test because it simulates exactly the workings of an actual trap. This test requires the SNMP message be correctly specified (including authentication credentials) and that Console's SNMPTrap Service is running.

NOTES:

1. Your client system must have SNMP access to the server to use the **Test response by sending an SNMP trap to ASM** level of testing.
2. The NetSight SNMPTrap Service (snmptrapd) must be configured with Security User credentials and/or Engine IDs for devices from which Console's SNMPTrap Service (snmptrapd) accepts SNMPv3 Notification messages. Without this information, notification messages are dropped by SNMPTrap Service. The traps do not appear in the Events view and ASM does not receive notification. Refer to How to Configure the SNMP Trap Service to learn more about configuring SNMPTrap Service.

- Test response by directly invoking ASM - This level bypasses the SNMP trap mechanism, sending the trap directly to ASM. ASM processes the threat as if it were received as a real SNMP trap message. If ASM is in Search and Respond mode, the configured action will be applied.

Specify parameters of test incident to be sent to ASM

Both levels of testing use these parameters. Your settings here define a simulated threat sent to ASM. You should specify parameters that match your settings for the Rule you are testing.

Sender ID

This is a unique identifier associated with the intrusion detection system that detected the security event.

Sender Name

The sender name being tested. This is a unique name associated with the intrusion detection system that detected the event. Sender Names are case sensitive.

Threat Category

The event category being tested. ASM's default event categories are ASM_ATTACK, ASM_COMPROMISE, ASM_INFORMATIONAL, and ASM_MISUSE. Event Category Names are case sensitive.

Signature

A signature provides a unique identifier for the threat being tested.

Threat IP

This is the IP address of the end station attached to the port where the threat is detected.

Specify additional parameters for sending SNMP trap

These parameters allow Console's SNMPTrap Service to receive a test trap and notify ASM of the threat. They allow more comprehensive testing that simulate the receipt of an actual trap by Console's SNMPTrap Service.

SNMPv3 User Name

The user name of the simulated user used for testing.

Authentication Type

The authentication method used for the inform (MD5 or SHA) message.

Authentication Password

The authentication password of the simulated user.

Privacy Type

The encryption method used for the inform (DES or None) message.

Privacy Password

The encryption password for the simulated user.

Trap Receiver

This is the system running the SNMPTrap Service.

Trap Sender

The system sending the SNMP trap.

Save Password (clear text)

When checked, the password information is saved as human readable text in the ASMClientOptions.properties file in the `<user's home directory>\NetSight\AutoSecMgr\Options` directory.

CAUTION: This feature is intended for use in a test environment and could present a security risk in your live network environment. It is recommended you do not select this option in a production environment.

Send Incident to ASM

Sends the test (inform) message you've configured to ASM. If you've configured your ASM Rules correctly, the message information appears in the ASM Monitor.

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Automated Security Manager Options
- Automated Security Manager Activity Monitor
- Traps and Informs

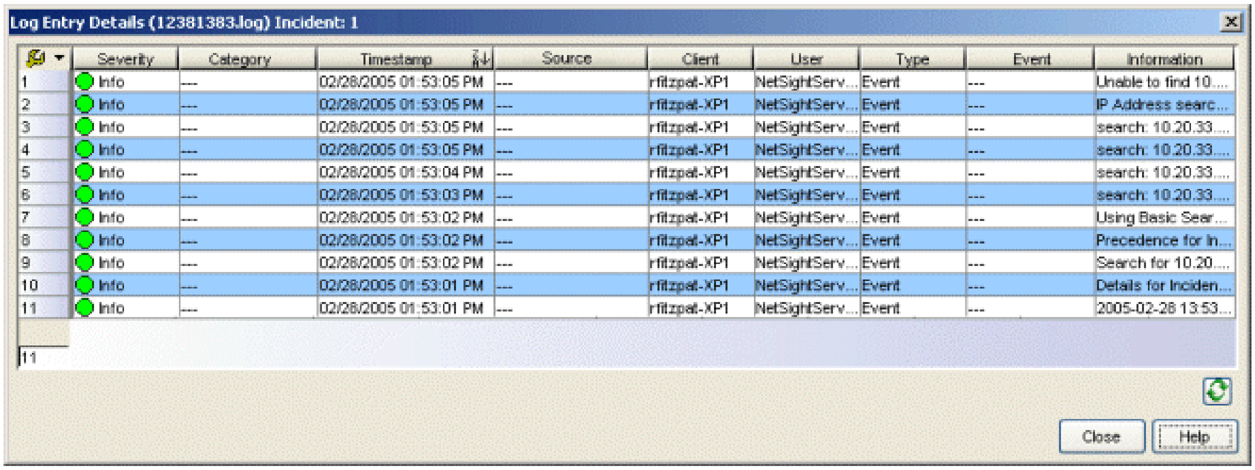
For information on related tasks:

- How to Set Automated Security Manager Options
- How to Create and Edit Automated Security Manager Rules
- How to Use Automated Security Manager Activity Monitor

ASM Log Entry Details Window

This window displays detailed information about a specific trap/action entry selected in the Automated Security Manager Activity Monitor. Activities related to the selected Activity Monitor entry are listed chronologically, by default, with newer activities at the bottom. You can change the arrangement by clicking a heading to sort the table in ascending or descending order. The Log Entry Details window is launched by double-clicking an entry in the Activity Monitor table or from the **View Details** option on the ASM Activity Monitor right-click menu.

Log details are maintained in date-stamped files in the `<install directory>\NetSight\appdata\logs` directory. A new file is opened each day. Entries in these files wrap around (overwrite the oldest information) when the file reaches its maximum size (1 Mb) and there is no automatic housekeeping to remove older files from this directory.



	Severity	Category	Timestamp	Source	Client	User	Type	Event	Information
1	● Info	---	02/28/2005 01:53:05 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	Unable to find 10....
2	● Info	---	02/28/2005 01:53:05 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	IP Address searc...
3	● Info	---	02/28/2005 01:53:05 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	search: 10.20.33....
4	● Info	---	02/28/2005 01:53:05 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	search: 10.20.33....
5	● Info	---	02/28/2005 01:53:04 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	search: 10.20.33....
6	● Info	---	02/28/2005 01:53:03 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	search: 10.20.33....
7	● Info	---	02/28/2005 01:53:02 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	Using Basic Sear...
8	● Info	---	02/28/2005 01:53:02 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	Precedence for In...
9	● Info	---	02/28/2005 01:53:02 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	Search for 10.20....
10	● Info	---	02/28/2005 01:53:01 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	Details for Inciden...
11	● Info	---	02/28/2005 01:53:01 PM	---	rfitzpat-XP1	NetSightServ...	Event	---	2005-02-28 13:53...

11

Severity
: Indicates the potential impact of the event.

Category
: For traps, this column shows the event category for the event.

Timestamp
: Shows the date and time when the event occurred.

Source
: Shows the IP address of the host that is the source of the event.

Client

Shows the hostname of the source of the event.

User

Associates an event with the user that performed the action that triggered the event.

Type

Identifies the type of information for this row (event or trap).

Event

Shows the type of event or trap.

Information

Shows an summary explanation of the event or trap.

Refresh

This button updates the table information.

Right-Click Menu

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

- Acknowledge Selected - places a check in the Acknowledge column for all of the selected rows.
- Unacknowledge Selected - removes the checks in the Acknowledge column from all of the selected rows.
- Acknowledge All - places a check in the Acknowledge column for all rows.
- Unacknowledge All - removes the checks in the Acknowledge column from all rows.
- Event Details - opens the Event Details window which provides additional information about a selected event or trap.

Related Information

For information on related windows:

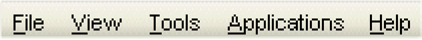
- ASM Configuration Window
- ASM Options
- Create/Edit Rule Window

For information on related tasks:

- How to Set ASM Options
- How to Create and Edit ASM Rules
- How to Use ASM Activity Monitor

Menu Bar

The ASM menu bar provides access to tools and functions that help you maintain the security of your network. ASM menus are available in several forms, designed for your convenience when accessed in a given situation. Many of the options available from menus are also available as buttons the toolbar. Icons associated with these menu options indicate when the same option is available from a toolbar. Specific menu options are dynamically enabled and disabled depending on which window, object, and tab is selected.



File Menu

Database > Initialize ASM Components

Initializes the ASM components in the current database, restoring them to the default settings as they existed immediately after installation. This option does not affect other Console database components.

Exit

Terminates an ASM session.

View Menu

Show Statistics Summary Panel

When checked, the Activity Monitor window presents the Statistics Summary panel.

Show Operational Mode Panel

When checked, the Activity Monitor window presents the Operational Mode panel.

Show Incident Filter

When checked, the Activity Monitor window presents the Incident Filter panel.

Tools Menu

Authorization/Device Access

Opens the Authorization/Device Access window where you can configure users and groups and control their access to features in NetSight applications.

Server Information

Opens the Server Information window where you can view and configure certain NetSight Server functions.

Incident Test Tool

Opens the ASM Incident Test Tool, where you can create a simulated trap message and send it to ASM to verify the response that you configure. This button is only active in **Search Only** and **Search and Respond** operational modes.

Modify snmptrapd.conf

Opens a text editor window, where you can define user credentials in the TrapService configuration file (snmptrapd.conf). Refer to snmptrapd.conf Text Editor Window more information about editing the snmptrapd.conf file.

ASM Configuration

Opens the Automated Security Manager Configuration window. The Configuration Window takes you step-by-step through configuring Automated Security Manager actions and targets. The window is dynamically updated as you set or change/define settings, always presenting the appropriate options as your configuration progresses. As you move through the steps, the selections that you make along the way determine the selections that are appropriate for the following steps.

Statistics

This option provides access to a submenu giving you selections that determine the statistics presented in the Activity Monitor window:

- **Configure** - opens the ASM Statistics window, where you can select the specific data elements to show in the Statistics Summary panel.
- **Reset Counters** - resets the counters for the accumulated data and sets the timestamp to the current date and time. Refer to the ASM Statistics window for a description of specific data elements.

- Show Summary Panel - when checked, displays the Statistics Summary as a panel in the upper half of the ASM Activity Monitor window.

Operational Mode

This option provides access to a submenu that controls ASM's operational mode:

- Show as Panel - when selected, displays a full Operational Mode panel in the ASM Activity Monitor window.
- Show as Icon - when selected, displays an iconized version of the Operational Mode panel as a *traffic light* in the upper-right corner of the ASM Activity Monitor window.
- Disabled - when selected, Automated Security Manager is not active. It neither seeks out the sources of network threats nor responds to them.
- Search Only - when selected, security threats are recognized, source ports are identified and the information is recorded in the Activity Monitor, but responses are not applied.
- Search and Respond - when selected, Automated Security Manager is fully active. In this state, threats are recognized, source ports are identified, and responses (actions) applied.

Options

Opens the Options window where you can set various parameters used by the Automated Security Manager.

Applications Menu

Lets you launch other NetSight applications from ASM.

Help Menu

Help Topics (Contents)

Opens the help browser to the Automated Security Manager Help System Welcome topic where you can access all of Automated Security Manager's online help topics.

Release Notes

Displays the NetSight Release Notes.

Support Center

Opens the Extreme Networks Support website.

Check for Updates

Allows you to update Automated Security Manager with the latest software patches. Refer to Suite-Wide Tools Web Update Help topic for more information.

Getting Started

Opens the Getting Started Help information to introduce first-time users to the features in NetSight Automated Security Manager.

About This Window

Displays help for the content currently displayed in the Main window.

About NetSight Automated Security Manager

Displays product information for the NetSight Suite.

Related Information

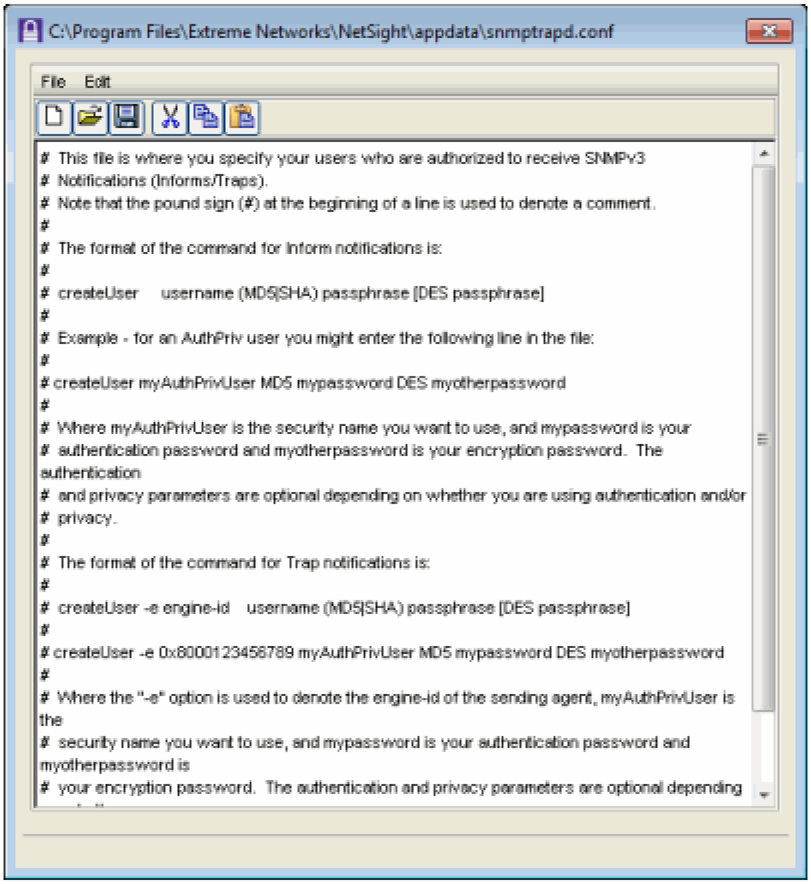
For information on related windows:

- Toolbar

snmptrapd.conf Text Editor Window

This window lets you edit the content of the snmptrapd.conf file to define credentials used by Console when receiving Inform messages. The File and Edit menus and toolbar provide facilities for editing and saving the snmptrapd.conf file. The SNMPTrap Service must be restarted after editing the file. For more information about Trap and Inform messages, refer to Traps and Informs.

Sample snmptrapd.conf file editor


C:\Program Files\Extreme Networks\NetSight\appdata\snmptrapd.conf
File
Edit

```
#  This file is where you specify your users who are authorized to receive SNMPv3
#  Notifications (Informs/Traps).
#  Note that the pound sign (#) at the beginning of a line is used to denote a comment.
#
#  The format of the command for Inform notifications is:
#
#  createUser     username (MD5|SHA) passphrase [DES passphrase]
#
#  Example - for an AuthPriv user you might enter the following line in the file:
#
# createUser myAuthPrivUser MD5 mypassword DES myotherpassword
#
#  Where myAuthPrivUser is the security name you want to use, and mypassword is your
#  authentication password and myotherpassword is your encryption password.  The
authentication
#  and privacy parameters are optional depending on whether you are using authentication and/or
#  privacy.
#
#  The format of the command for Trap notifications is:
#
#  createUser -e engine-id    username (MD5|SHA) passphrase [DES passphrase]
#
# createUser -e 0x8000123456789 myAuthPrivUser MD5 mypassword DES myotherpassword
#
#  Where the "-e" option is used to denote the engine-id of the sending agent, myAuthPrivUser is
the
#  security name you want to use, and mypassword is your authentication password and
myotherpassword is
#  your encryption password.  The authentication and privacy parameters are optional depending
```

You can define security information for Inform messages using the `createUser` directive in the `snmptrapd.conf` file. Add one createUser directive for each Security User: **`createUser`**

Example for Informs:

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

Where:	
myUser	security user name
myauthpassword	`MD5` or `SHA` - authentication type and authentication password (optional parameter - do not use when authentication is not used)
myprivpassword	`DES` - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

Any time the snmptrapd.conf file is changed, the SNMPTrap Service must be restarted.

Restarting snmptrapd Service

Depending on the system where the NetSight Server is running and your preference, there are several ways to restart the snmptrapd service.

Restarting the service locally on the NetSight Server host system

Windows

Using the Services Manager:

1. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar).
2. Locate the Services Manager icon (E) and right-click it.
3. Select **SNMPTrap** > **Restart**.

Using Windows Services:

1. From the Control Panel, access the Administrative Tools > Services window.
2. Locate the snmptrapd service and select "Restart the service."

Linux

1. Navigate to the `etc/init.d` directory.
2. Type the command:
   ```
   nssnmptrapd stop
   ```
3. Press **Enter**.

4. Type the command:
   `nssnmptrapd start`
5. Press **Enter**.

Restarting the service remotely from a NetSight Client host system

Windows

Restarting the service remotely on Windows host systems is only possible if both the Client and Server are capable of running **Remote Desktop** (a feature of Windows XP Professional) or through the use of a third-party facility that provides similar capabilities to Remote Desktop.

When you can access the Services Manager on the remote system using either Remote Desktop or a third-party program, you can restart the service as follows:

1. Go to the Taskbar Notification Area of the remote desktop.
2. Locate the Services Manager and right click the icon (▣).
3. Select **SNMPTrap** > **Restart**.

Linux

1. Telnet to the server and login as an administrative user.
2. Navigate to the `etc/init.d` directory.
3. Type the command:
   `nssnmptrapd stop`
4. Press **Enter**.
5. Type the command:
   `nssnmptrapd start`
6. Press **Enter**.
7. Log out and close the telnet session.

Related Information

For information on related windows:

- Automated Security Manager Options
- Automated Security Manager Activity Monitor

For information on related tasks:

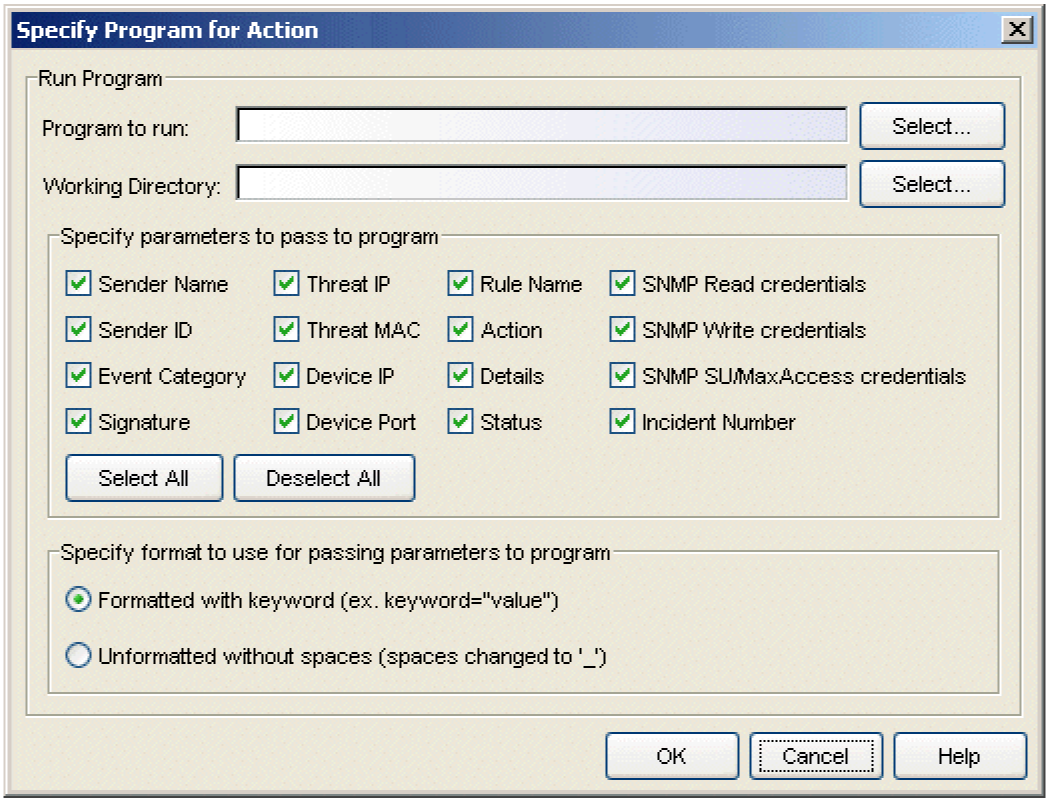
- How to Set Automated Security Manager Options
- Using the Automated Security Manager Activity Monitor

Specify Program for Action/Undo Window

When creating a rule, this window lets you:

- customize the response to an event by selecting a program to be executed (Specify Program for Action)
- specify an action taken when a rule action is undone (Specify Program for Undo)

In either case, the information you configure is the same for both windows, the only difference is the title of the window. The window is accessed from the ASM Configuration Window's Rule Definitions view.



Specify Program for Action

Run Program

Program to run:

Working Directory:

Specify parameters to pass to program

☑ Sender Name	☑ Threat IP	☑ Rule Name	☑ SNMP Read credentials
☑ Sender ID	☑ Threat MAC	☑ Action	☑ SNMP Write credentials
☑ Event Category	☑ Device IP	☑ Details	☑ SNMP SU/MaxAccess credentials
☑ Signature	☑ Device Port	☑ Status	☑ Incident Number

Specify format to use for passing parameters to program

● Formatted with keyword (ex. keyword="value")

○ Unformatted without spaces (spaces changed to '_')

Program to run

This field defines the script launched for this Custom Action or Custom Undo. Scripts are stored in the <install directory>\NetSight\appdata\AutoSecMgr\scripts directory. Type a script name, if known, or use the **Select** button to open a file browser window and choose a script.

You can not use options with the Program to run field. For example, you cannot enter `myscript.bat -i <IP Address> -m <MAC Address>` in the Program to run field.

TIP: To execute a script with options, create a script without options that executes another script with options (Windows only). For example:

1. Create a script named, `asm_script.bat` with an entry to call `myscript.bat` such as:

   C:\Program Files\My Custom Files\myscript.bat -i %1 -m %2".
2. Uncheck all but the **Threat IP** and **Threat MAC** checkboxes and select **Unformatted without spaces** (you don't want to send any keyword (thip= or thmac=) to your script.). The variable %1 returns <*Threat IP Address*> and %2 returns the <*Threat MAC Address*>.

   If you are using PERL script, use a different argument variable, such as $ARGV[0] (First argument) or @ARGV (all arguments). Also, using the shell script is similar to a Windows batch file script (%1 for the first argument, %* for the all arguments).

Working Directory

This is the path to the directory from which the script is executed. Any path references within your script that are not absolute paths, are relative to this directory. Enter a path or use the Select button to open a file browser window and choose a directory.

Specify parameters to pass...

These check boxes let you select elements of the event information that are passed as parameters to your program. The Select All button places a check in all of the boxes and the Deselect All button removes checks from all of the boxes.

Specify format to use...

This area lets you select the format used to pass the selected parameters to your program:

Formatted with keyword...

When selected, the parameters are passed using a format that includes a keyword associated with each parameter (e.g., **`keyword="value"`**). So, for example, if Sender Name is selected as a parameter, the keyword sname is used and the information passed to the script is **`sname="dragon_id"`** followed by a space and then the keyword and value for the next parameter. The following table defines the keywords for each parameter and the order that the values are passed to the script (listed from top to bottom in the table).

Parameter	Keyword
Sender Name	sname
Sender ID	sid
Event Category	ecat
Signature	sig
Incident Number	incident
Threat IP	thip
Threat MAC	thmac
Device IP	dev
Device Port	port
Rule Name	rname
Action	action
Details	dtls
SNMP Parameters	see Note 1
Status	stat

Note 1: When you select any SNMP parameter, the **`snmp=`***value* indicates the SNMP version and the subsequent parameters contain the values assigned for the credentials associated with the device. When you select multiple SNMP parameters (e.g., SNMP Write and SNMP Read) the script uses the values for the highest access level.

SNMP v1, SNMPv2		SNMPv3	
Parameter	**Keyword**	**Parameter**	**Keyword**
SNMP Read	snmp="v1" ro	SNMP Read, SNMP Write, SNMP SU/Max Access	snmp="v3" user seclevel authtype authpwd privtype privpwd
SNMP Read	snmp="v1" rw		
SNMP Read	snmp="v1" su		

Example:

If you select Sender Name, Sender ID, Threat MAC, and SNMP Write and the device is configured for SNMPv1 credentials, the information passed to the script appears as:

```
sname="my sender name" sid="dragon id"
thmac="00.00.1d.11.22.33" snmp="v1" rw="public"
```

And, for a script named **myscript.bat**, the resulting script command is executed as:

```
<install directory>\NetSight\appdata\AutoSecMgr\scripts\m
y_script.bat sname="my sender name" sid="dragon id"
thmac="00.00.1d.11.22.33" snmp="v1" rw="public"
```

Unformatted without spaces...

When selected, the parameters are passed as space delimited, unformatted text, without keywords. For this option, your script must know which parameters are being passed and the order in which they are passed. If a parameter contains any spaces, they are replaced with an underscore (_).

Example:

You select Sender Name, Sender ID, Threat MAC, and SNMP Write and the device is configured for SNMPv1 credentials, the information passed to the script appears as:

```
my_sender_name dragon_id 00.00.1d.11.22.33 v1 public
```

And, for a script named **myscript.bat**, the resulting script command is executed as:

```
<install directory>\NetSight\appdata\AutoSecMgr\scripts\m
y_script.bat my_sender_name dragon_id 00.00.1d.11.22.33 v1
public
```

Related Information

For information on related windows:

- Automated Security Manager Configuration Window
- Create/Edit Rule Window

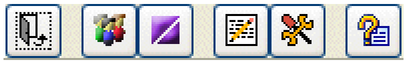
For information on related tasks:

- How to Create and Edit Automated Security Manager Rules
- Usng the Automated Security Manager Activity Monitor

Toolbar

The ASM toolbar provides easy access to some of the more commonly used Automated Security Manager menu functions. Some Toolbar buttons may not be available, depending on your current selection within ASM. Pausing with your mouse pointer over toolbar icons displays tool tips showing each button's function.

The Toolbar offers the following shortcuts to frequently used menu selections:



Exit

Exits the application.

Authorization/Device Access

Opens the Authorization/Device Access window, where you can configure users and groups and control their access to features in NetSight applications.

Server Information

Opens the Server Information window, where you can view and configure certain NetSight Server functions.

Incident Test Tool

This button opens the ASM Incident Test Tool, where you can create a simulated trap message and send it to ASM to verify the response that you've configured. This button is only active in **Search Only** and **Search and Respond** operational modes.

ASM Configuration

Opens the Automated Security Manager Configuration window. The Configuration Window takes you step-by-step through configuring Automated Security Manager actions and targets. The window is dynamically updated as you set or change/define settings, always presenting the appropriate options as your configuration progresses. As you move through the steps, the selections that you make along the way determine the selections that are appropriate for the following steps.

Help - About This Window

Displays help for the content currently displayed in the main window.

Reference Information

The **References** section contains information referenced by other Help topics.

Disable Log Entry Details

If you experience ASM performance problems while under extreme network load, you can improve performance by disabling Log Entry Details. The Log Entry Details window displays information about a specific trap/action entry in the Automated Security Manager Activity Monitor, and can be useful for debugging purposes. The window is launched by double-clicking an entry in the Activity Monitor table.

To disable Log Entry Details, edit your ASM properties file as follows:

1. Navigate to the Properties file: <install directory>\NetSight\appdata\AutoSecMgr\AutoSecMgr.properties
2. Open the AutoSecMgr.properties file in a text editor and add the following lines:
   ```
   #asm.logging.summary.useTopic=false
   #asm.logging.summary.enabled=false
   asm.logging.detail.useTopic=false
   asm.logging.detail.enabled=false
   ```
3. If you still have performance problems, you can disable all logging by uncommenting the two lines that control summary logging. Summary logging refers to the events logged in the Automated Security Event Log tab.

MIB/Table Descriptions

This topic provides a brief description of the data sources and MIB objects specified as search filters when configuring ASM Search Variables.

Node/Alias (ctAlias)

This MIB defines objects used to discover end-systems per port and to map end-system addresses to the layer 2 address of the port. Select this MIB to resolve IP addresses to MAC addresses when the devices in your network support the Node/Alias (ctAlias) MIB.

IpRouteTable

An entity's IP Routing table. This selection provides the ability to resolve IP addresses to MAC addresses. Select this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). Include your routers in your search scope when this MIB is selected.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

IpCIDRRouteTable

The IP CIDR Route Table replaces the now obsolete ipRoute Table current in MIB-I and MIB-II and the IP Forwarding Table . It adds knowledge of the autonomous system of the next hop, multiple next hops, and policy routing, and Classless Inter-Domain Routing. Select this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). Include your routers in your search scope when this MIB is selected.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

ipNetToMedia

IP Address Translation table used for mapping from IP addresses to physical addresses. This table is read whenever an entry is found by IP Route or IP CIDR Route searches, regardless of whether you select the IPNetToMedia. Selecting the IPNetToMedia checkbox only affects whether or not the entire IPNetToMedia table is read. Select this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). Include your routers in your search scope when this MIB is selected.

This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

Dot1dTpFdb

This table contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame. Select this MIB to resolve MAC addresses to a port.

Dot1qTpFdb

This table contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame. Select this MIB to resolve MAC addresses to a port.

Dot1qVLAN Current

This table contains current configuration information for each VLAN currently configured into the device by (local or network) management, or dynamically created as a result of GVRP requests received. Select this MIB to resolve MAC addresses to a port.

802.1XAuthentication (PAE)

Port Access Entity module for managing IEEE 802.1X

Enterasys 802.1X Extensions

Supplements/used in connection with the standard IEEE 802.1x MIB. It provides a convenient way to retrieve authentication status for supplicants living on shared-media ports that use station-based access control. (Here, a MAC address is a much more natural table index than a port or interface number.)

Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys Port Web Authentication (PWA)

Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys MAC Locking

Provides configuration and status objects pertaining to per port MAC Locking. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys MAC Authentication

Used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys Multiple Authentication

Used for authentication using multiple authentication mechanisms. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys IGMP MIB

Extends the Standard IGMP MIB for configuration of IGMP on Enterasys devices. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

IGMP Standard

MIB module for IGMP Management, it contains an IGMP Interface Table with one row for each interface on which IGMP is enabled and an IGMP Cache Table with one row for each IP multicast group for which there are members on a particular interface. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

RMON addressMap

MAC address to network address bindings discovered by the probe and shows the interface on which they were last seen. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

RMON host table

Contains entries for each address discovered on a particular interface. Each entry contains statistical data about that host. This table is indexed by the MAC address of the host, through which a random access may be achieved. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys Multiple User 802.1X

This MIB contains information pertaining to Multi-User IEEE 802.1X authentication and supplements the standard IEEE 802.1X-2001 MIB. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Enterasys Convergence End Point

This table contains information for each of the Convergence End Points discovered or detected on your network. Select this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so selecting this MIB is usually not necessary.

Traps and Informs

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

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

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

SNMPv3 Traps

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

Because of this, you must define the Security User credentials and engineID of the SNMP agents for every device from which you want to receive SNMPv3 traps. This information is defined using the `createUser` directive in the `snmptrappd.conf` file. So, if you want to have 100 SNMP agents send SNMPv3 traps to the SNMPTrap Service, you need 100 `createUser` directives (defining both the security user credentials and engine ids) in the configuration file.

`createUser` Example for Traps:

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

Where:	
`-e` *<engine:id>*	Specifies the engineID of the sending agent.
myUser	Security user name.
myauthpassword	`MD5` or `SHA` - authentication type and authentication password (optional parameter - do not use when authentication is not used).
myprivpassword	`DES` - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

SNMPv3 Informs

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

The `createUser` directive in the `snmptrapd.conf` file defines security information for Inform messages.

`createUser` Example for Informs:

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

Where:	
myUser	Security user name.
myauthpassword	`MD5` or `SHA` - authentication type and authentication password (optional parameter - do not use when authentication is not used).
myprivpassword	`DES` - encryption type and encryption password - (optional parameter - do not use when encryption is not used or leave the encryption password blank if it is the same as the authentication password).

Restart the SNMPTrap Service

Any time you change the snmptrapd.conf file, the SNMPTrap Service must be restarted.

To restart the snmptrapd:

Windows	Linux
a. Go to the Taskbar Notification Area of your desktop (on the lower right of your screen, unless you've relocated your Taskbar). b. Right-click the Services Manager icon (▣). c. Select **SNMP Trap** > **Restart**.	a. Navigate to the `etc/init.d` directory. b. Type the command: `nssnmptrapd stop` c. Press **Enter**. d. Type the command: `nssnmptrapd start` e. Press **Enter**.

Remote ASM Undo

This Help topic provides instructions on how to remotely undo an ASM action by sending an SNMPv3 inform message to the ASM trap server. This can be useful in networking environments where network operations people who do not have access to ASM need to be able to remotely undo an ASM action. With the remote ASM undo, operations people can remove an end user from the Quarantine state by sending an SNMPv3 inform, allowing the end user to regain normal access to the network without requiring assistance from network administrators and ASM.

The first section provides instructions on gathering the information needed for the inform message. The second section provides steps for using the SNMP trap utility to send the inform message to the ASM trap server.

Preparing the Inform Message

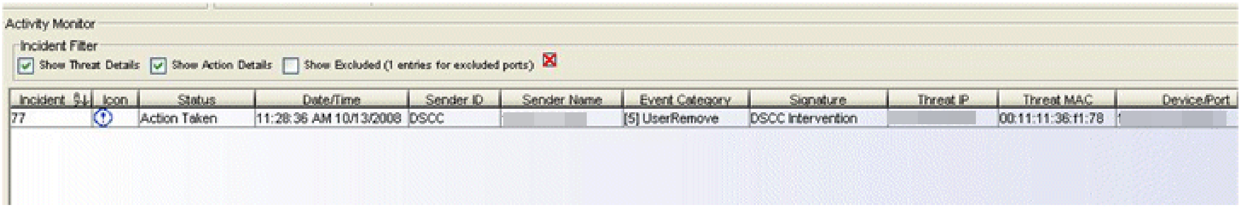
The inform message consists of SNMP credentials and the following six parameters:

- etsysThreatUndoNotificationMessage (1.3.6.1.4.1.5624.1.2.45.1.0.5)
  Identifies the inform message as a Threat Undo Notification.
- etsysThreatNotificationIncidentID (1.3.6.1.4.1.5624.1.2.45.1.1.14)
  The ASM incident number assigned to the threat.
- etsysThreatNotificationDeviceAddress (1.3.6.1.4.1.5624.1.2.45.1.1.6)
  The IP address of the device where the threat is detected.
- etsysThreatNotificationDeviceIfIndex (1.3.6.1.4.1.5624.1.2.45.1.1.7)
  The IfIndex value of the port where the threat is detected.
- etsysThreatNotificationInitiatorAddress (1.3.6.1.4.1.5624.1.2.45.1.1.9)
  The IP address of the device that is the source of the threat.
- etsysThreatNotificationInitiatorMacAddress (1.3.6.1.4.1.5624.1.2.45.1.1.13)
  The MAC address of the device that is the source of the threat.

You need to provide values for the last five parameters listed above. You can view values for four of the five parameters in the ASM Activity Monitor in ASM Manager, as shown in the image below.

- etsysThreatNotificationIncidentID
  The number listed in the Incident column.

- etsysThreatNotificationDeviceAddress
  The IP address listed in the Device/Port column.
- etsysThreatNotificationInitiatorAddress
  The IP address listed in the Threat IP column.
- etsysThreatNotificationInitiatorMacAddress
  The MAC address listed in the Threat MAC column.



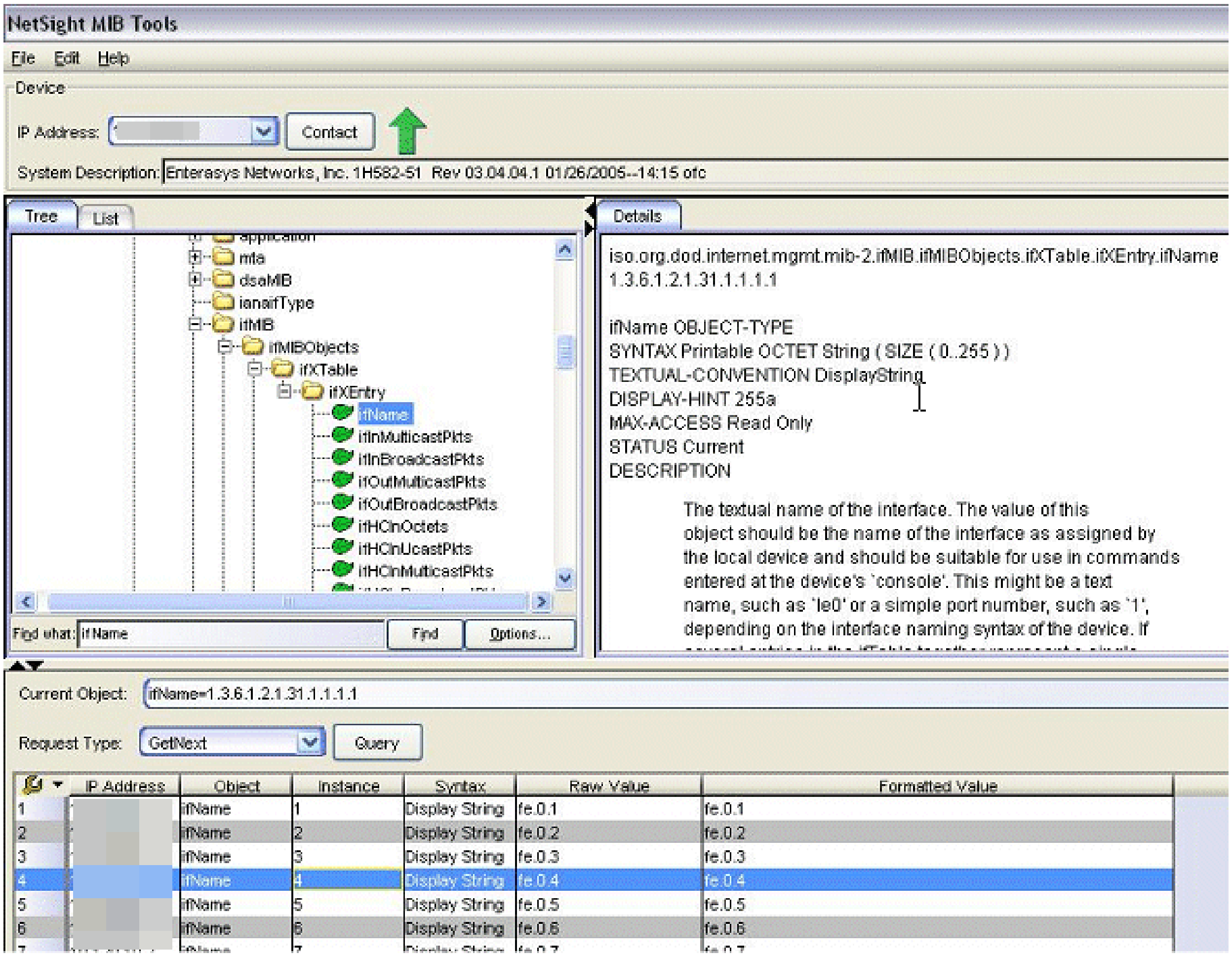
Activity Monitor

Incident Filter

☑ Show Threat Details ☑ Show Action Details □ Show Excluded (1 entries for excluded ports) ☒

Incident	Icon	Status	Date/Time	Sender ID	Sender Name	Event Category	Signature	Threat IP	Threat MAC	Device/Port
77	ⓘ	Action Taken	11:28:36 AM 10/13/2008	DSCC	[redacted]	[5] UserRemove	DSCC Intervention	[redacted]	00:11:11:36:f1:78	[redacted]

You must determine the etsysThreatNotificationDeviceIfIndex parameter value using a MIB browser tool such as NetSight MIB Tools. The ifName MIB (1.3.6.1.2.1.31.1.1.1.1) contains the interface name of all the ports on a device. Each interface name has a unique instance value that is also its ifIndex. In the example above, the IP address of the device that detected the threat is 10.120.10.2 and the port the threat is detected on is fe.0.4. If we use MIB Tools to query the ifName MIB on 10.120.10.2, the query results show that port fe.0.4 has an instance value of 4. This is the ifIndex value used in the inform message.



IP Address: [redacted]

System Description: Enterasys Networks, Inc. 1H582-51 Rev 03.04.04.1 01/26/2005--14:15 ofc

Find what: ifName

iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName
1.3.6.1.2.1.31.1.1.1.1

ifName OBJECT-TYPE
SYNTAX Printable OCTET String (SIZE (0..255))
TEXTUAL-CONVENTION DisplayString
DISPLAY-HINT 255a
MAX-ACCESS Read Only
STATUS Current
DESCRIPTION

The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `le0' or a simple port number, such as `1', depending on the interface naming syntax of the device. If

Current Object: ifName=1.3.6.1.2.1.31.1.1.1.1

Request Type: GetNext

	IP Address	Object	Instance	Syntax	Raw Value	Formatted Value
1	[redacted]	ifName	1	Display String	fe.0.1	fe.0.1
2	[redacted]	ifName	2	Display String	fe.0.2	fe.0.2
3	[redacted]	ifName	3	Display String	fe.0.3	fe.0.3
4	[redacted]	ifName	4	Display String	fe.0.4	fe.0.4
5	[redacted]	ifName	5	Display String	fe.0.5	fe.0.5
6	[redacted]	ifName	6	Display String	fe.0.6	fe.0.6
7	[redacted]	ifName	7	Display String	fe.0.7	fe.0.7

Using the SNMP Trap Utility to Undo the ASM Action

Use the following steps to undo an ASM action with the SNMP trap utility using the inform message.

1. Open a command prompt window and "cd" to the following directory that contains the SNMP trap utility.

   ```
   <install directory>\NetSight\tools\ucdutils.
   ```

   TIP: To view all the SNMP trap options, display the help information by typing "snmptrap -h".

2. Enter the following command:

   ```
   snmptrap -C i -v3 -u <username> -a <authentication type> -
   ```

```
A <authentication password> -x <privacy type> -X <privacy
password> <trap server IP> 0
.1.3.6.1.4.1.5624.1.2.45.1.0.5
.1.3.6.1.4.1.5624.1.2.45.1.1.14 i <incident>
 .1.3.6.1.4.1.5624.1.2.45.1.1.6 s <device
IP>.1.3.6.1.4.1.5624.1.2.45.1.1.7 i <port ifIndex>
 .1.3.6.1.4.1.5624.1.2.45.1.1.9 s <threat IP>
 .1.3.6.1.4.1.5624.1.2.45.1.1.13 x <threat MAC>
```

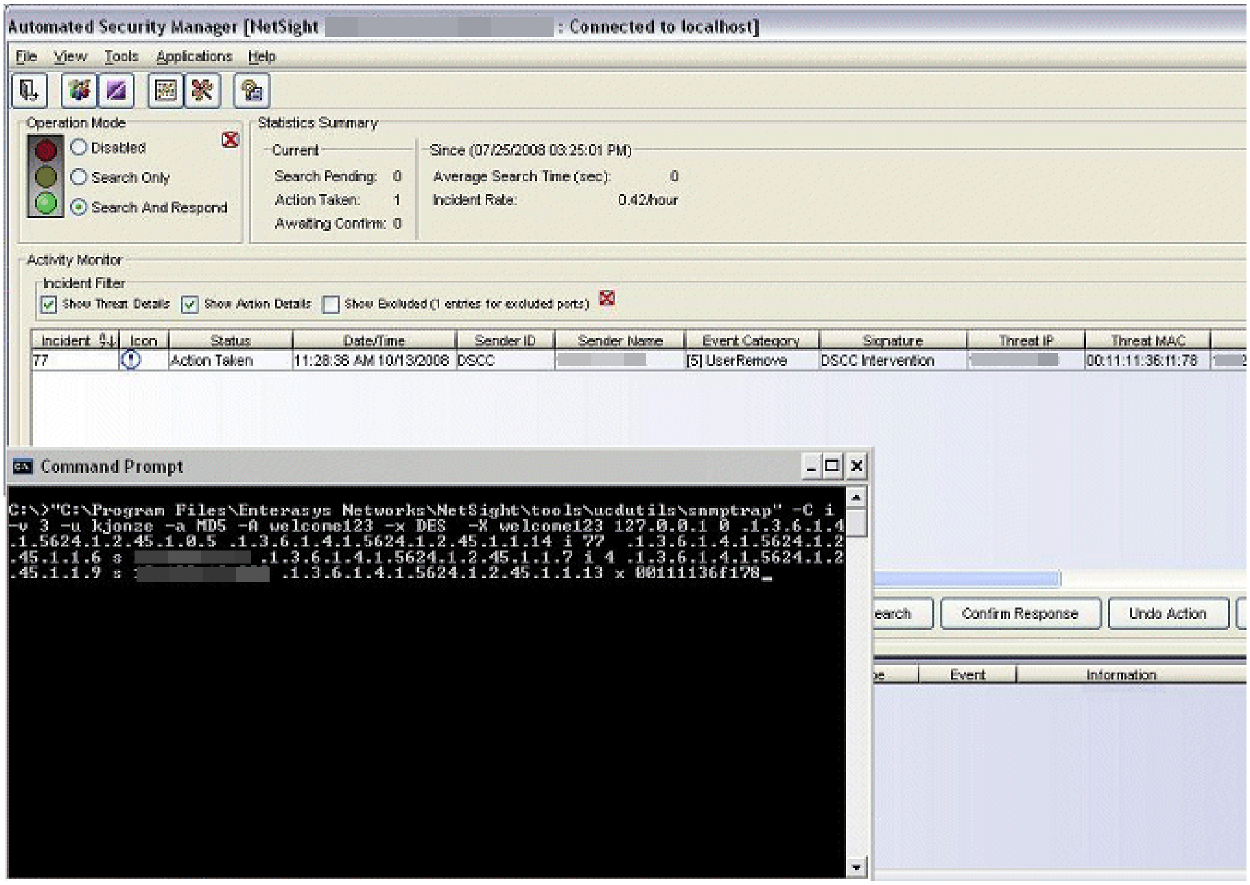
In the command, enter the SNMPv3 credentials and the appropriate values for the parameters. Replace <trap server IP> with the IP address of the PC/server running ASM. Replace <incident>, <device IP>, <threat IP>, and <threat MAC> with the values from the ASM Activity Monitor. You must enter the <threat MAC> value with no delimiters (e.g., no colons). Replace <port ifIndex> with the correct port ifIndex number obtained from the MIB query.

Here is an example of what the command looks like using the values displayed in the ASM Activity Monitor and MIB Tools examples above:

```
snmptrap -C i -v 3 -u kjonze -a MD5 -A welcome123 -x DES -
X welcome123 127.0.0.1 0 .1.3.6.1.4.1.5624.1.2.45.1.0.5
.1.3. 6.1.4.1.5624.1.2.45.1.1.14 i 77
.1.3.6.1.4.1.5624.1.2.45.1.1.6 s 10.120.10.2
.1.3.6.1.4.1.5624.1.2.45.1.1.7 i 4 .1.
3.6.1.4.1.5624.1.2.45.1.1.9 s 10.120.10.200
.1.3.6.1.4.1.5624.1.2.45.1.1.13 x 00111136f178
```

3. Press **Enter** to send the snmptrap command to the trap server.

The following image shows an example of the ASM Activity Monitor prior to sending the snmptrap command. You can see that the action is taken (Status column) and the Event View received no SNMP inform messages.



Automated Security Manager [NetSight [redacted] : Connected to localhost]

Operation Mode

○ Disabled
○ Search Only
● Search And Respond

Statistics Summary

Current
Search Pending: 0
Action Taken: 1
Awaiting Confirm: 0

Since (07/25/2008 03:25:01 PM)
Average Search Time (sec): 0
Incident Rate: 0.42/hour

Activity Monitor

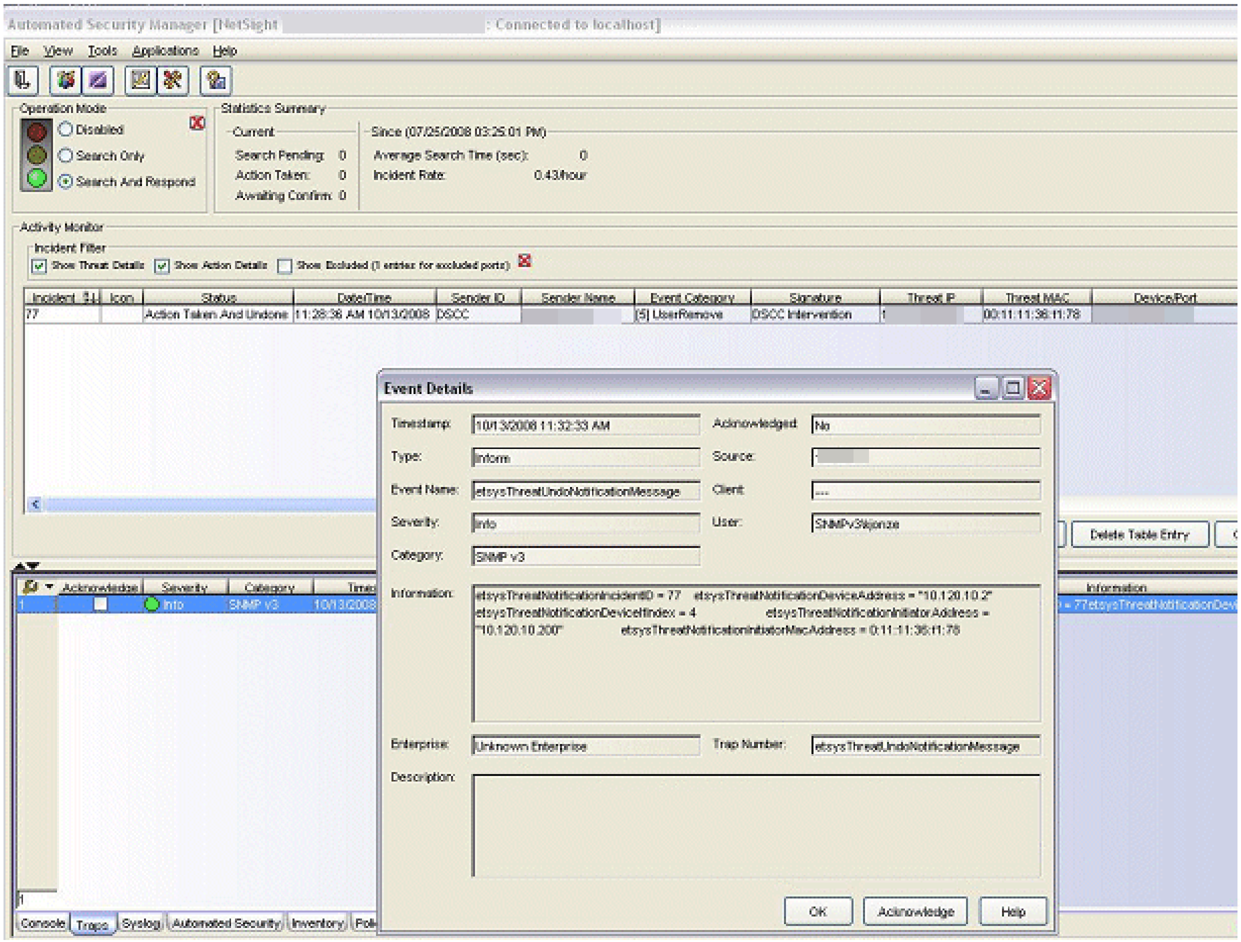
Incident Filter
☑ Show Threat Details ☑ Show Action Details □ Show Excluded (1 entries for excluded ports)

Incident	Icon	Status	Date/Time	Sender ID	Sender Name	Event Category	Signature	Threat IP	Threat MAC	
77	ⓘ	Action Taken	11:28:38 AM 10/13/2008	DSCC	[redacted]	[5] UserRemove	DSCC Intervention	[redacted]	00:11:11:36:f1:78	[redacted]

Command Prompt

```
C:\>"C:\Program Files\Enterasys Networks\NetSight\tools\ucdutils\snmptrap" -C i
-v 3 -u kjonze -a MD5 -A welcome123 -x DES  -X welcome123 127.0.0.1 0 .1.3.6.1.4
.1.5624.1.2.45.1.0.5 .1.3.6.1.4.1.5624.1.2.45.1.1.14 i 77  .1.3.6.1.4.1.5624.1.2
.45.1.1.6 s [redacted] .1.3.6.1.4.1.5624.1.2.45.1.1.7 i 4 .1.3.6.1.4.1.5624.1.2
.45.1.1.9 s [redacted] .1.3.6.1.4.1.5624.1.2.45.1.1.13 x 00111136f178_
```

The next image shows the ASM Activity Monitor after sending the snmptrap command. You can see the action is undone (Status column) and the trap server received the SNMP inform message. Double-click on the inform event in the Event View to open the Event Details window.


Automated Security Manager [NetSight [redacted] : Connected to localhost]
File View Tools Applications Help
Operation Mode
Statistics Summary
Activity Monitor
Incident Filter
Delete Table Entry
Acknowledge Severity Category Time Information
Console Traps Syslog Automated Security Inventory Poli
Event Details
OK Acknowledge Help

Operation Mode: ○ Disabled ○ Search Only ● Search And Respond

Current
Search Pending: 0
Action Taken: 0
Awaiting Confirm: 0

Since (07/25/2008 03:25:01 PM)
Average Search Time (sec): 0
Incident Rate: 0.43/hour

☑ Show Threat Details ☑ Show Action Details □ Show Excluded (1 entries for excluded ports)

Incident	Icon	Status	Date/Time	Sender ID	Sender Name	Event Category	Signature	Threat IP	Threat MAC	Device/Port
77		Action Taken And Undone	11:28:38 AM 10/13/2008	DSCC	[redacted]	[5] UserRemove	DSCC Intervention	[redacted]	00:11:11:36:11:78	[redacted]

	Acknowledge	Severity	Category	Time	Information
1	□	Info	SNMP v3	10/13/2008	= 77etsysThreatNotificationDev

Event Details

Timestamp: 10/13/2008 11:32:33 AM
Acknowledged: No
Type: Inform
Source: [redacted]
Event Name: etsysThreatUndoNotificationMessage
Client: ---
Severity: Info
User: SNMPv3kjonze
Category: SNMP v3
Information: etsysThreatNotificationIncidentID = 77 etsysThreatNotificationDeviceAddress = "10.120.10.2" etsysThreatNotificationDeviceIfIndex = 4 etsysThreatNotificationInitiatorAddress = "10.120.10.200" etsysThreatNotificationInitiatorMacAddress = 0:11:11:36:11:78
Enterprise: Unknown Enterprise
Trap Number: etsysThreatUndoNotificationMessage
Description: