



Using External Monitoring, Troubleshooting, and Diagnostic Tools

A high degree of network availability is a requirement for large enterprises and service providers. Network managers face various challenges in maintaining network availability, including unscheduled down time, lack of expertise, insufficient tools, complex technologies, business consolidation, and competing markets. Network monitoring, problem diagnosis, and troubleshooting are essential to meeting and overcoming these challenges.

Monitoring involves the study of network activity and device status to identify anomalous events and behaviors. Quickly diagnosing and correcting network and system faults such as outages and degradations increase service availability, and thus tools to isolate, analyze and correct problems are essential.

The main Security Manager tools for monitoring device events are the Health and Performance Monitor (see [Chapter 70, “Health and Performance Monitoring”](#)) and the Event Viewer (see [Chapter 68, “Viewing Events”](#)).

In addition to Health and Performance Monitor and Event Viewer, the following topics describe additional monitoring, troubleshooting and diagnostic tools that are available with Security Manager:

- [Dashboard Overview, page 71-1](#)
- [CSM Mobile, page 71-11](#)
- [Viewing Inventory Status, page 71-12](#)
- [Starting Device Managers, page 71-14](#)
- [Launching Cisco Prime Security Manager or FireSIGHT Management Center, page 71-20](#)
- [Analyzing an ASA or PIX Configuration Using Packet Tracer, page 71-23](#)
- [Analyzing Connectivity Issues Using the Ping, Trace Route, or NS Lookup Tools, page 71-25](#)
- [Using the Packet Capture Wizard, page 71-30](#)
- [IP Intelligence, page 71-33](#)
- [Integrating CS-MARS and Security Manager, page 71-36](#)

Dashboard Overview

Beginning with Version 4.5, the Security Manager client has a new launch point—a configurable dashboard, for which this topic presents an overview.

The dashboard is one of the six client applications that you can select as your default client application when you start the Security Manager client. (The others are Configuration Manager, Event Viewer, Report Manager, Health and Performance Manager, and Image Manager; there is also an application designed for mobile devices called CSM Mobile.) The dashboard is a convenient way for you to accomplish tasks that are found in several other areas of Security Manager, such as the IPS Health Monitor page, Report Manager, Health and Performance Monitor, and IP Intelligence Settings.

The dashboard contains the widgets shown in the following table, categorized by whether they are for use with IPS, firewalls, or both. (Not all of these widgets are shown by default). In addition to the original dashboard, you can create new, additional dashboards, which are displayed as tabs. You can customize all dashboards, both the original dashboard and any new, additional dashboards that you create. To customize a dashboard, you can drag and drop widgets from the list of available widgets into any dashboard.

Table 71-1 Widgets for IPS, Firewalls, and Both

Widgets for IPS	<ul style="list-style-type: none"> • IPS Inspection Load Trends • Top 10 Reports for IPS Attackers, Victims, and Signatures • IPS Missed Packet Trends • IPS License • IPS Update Packages • IPS Sensors Out of Date
Widgets for Firewalls	<ul style="list-style-type: none"> • Top 10 Reports for Firewall Sources, Destinations, and Services • Top 10 Reports for Botnet Malware Sites, Ports, and Hosts • Firewall CPU Usage Trends
Widgets for Both IPS and Firewalls	<ul style="list-style-type: none"> • Device Health Summary • Memory Usage Trends • Deployment • IP Intelligence

The way in which you use the dashboard and its widgets depends upon your goals in using Security Manager. For example, you can use the following four widgets to observe device health trends:

- IPS Inspection Load Trends
- IPS Missed Packet Trends
- Memory Usage Trends
- Firewall CPU Usage Trends

Individual widgets are described in the following table. One of the key widgets is the Device Health Summary widget. One reason it is important is that it provides the same information accessible through CSM Mobile, which is designed specifically for mobile devices. For more information about CSM Mobile, see [CSM Mobile, page 71-11](#). For information on enabling or disabling CSM Mobile, see [CSM Mobile Page, page 11-9](#).

Table 71-2 *Description of Individual Widgets*
Dashboard widgets for IPS in Dashboard widgets for firewall in dashboard

IPS Inspection Load Trends	<p>A measure of the IPS inspection load trends. The inspection load trend data will appear in this widget only when an IPS device issues an alert because of inspection load, and the data will disappear when the alert is cleared.</p> <p>Indicates how much traffic inspection capacity the sensor is using. 0 indicates that there is no traffic backup, and 100 indicates that the buffers are completely backed up. Inspection load trends are affected by the following things:</p> <ul style="list-style-type: none"> • Rate of traffic that needs inspection • Type of traffic being inspected • Number of active connections being inspected • Rate of new connections per second • Rate of attacks being detected • Signatures active on the sensor • Custom signatures created on the sensor <p>You can set monitoring parameters on the IPS Health Monitor page at [IPS device in Device View] Platform > Device Admin > Health Monitor.</p>
-----------------------------------	--

Table 71-2 Description of Individual Widgets
Dashboard widgets for IPS in Dashboard widgets for firewall in dashboard (Continued)

Top 10 Reports for IPS Attackers, Victims, and Signatures	<p>Pre-defined system reports that you can use to analyze top attackers, victims, and signatures for IPS alerts in your network.</p> <p>Clickable Link—In the Top Attackers widget, the IP address is an active hyperlink; click it to display IP intelligence. For details on IP intelligence in Security Manager, refer to IP Intelligence, page 71-33.</p> <p>Clickable Link—In the Top Signatures widget, the Signature ID is an active hyperlink; click it to display signature information.</p> <p>To use these reports, use Report Manager (Launch > Report Manager...).</p> <p>To cross-launch Event Viewer from one of these top ten reports, select a particular attacker, victim, or signature, and click the number of occurrences. The number of occurrences is listed for the last 24 hours by default; you can change it to the last hour if desired.</p> <p>Note When you cross-launch Event Viewer, the event query time in Event Viewer will be shown as the last 10 minutes despite its being the last 24 hours or the last hour in the Summary Dashboard. You can change the event query time in Event Viewer from the last 10 minutes to another value by using the dropdown list.</p>
IPS Missed Packet Trends	<p>A measure of the IPS missed packets trends. The missed packets trend data will appear in this widget only when there is an alert based on missed packets, and the data will disappear when the alert is cleared.</p> <p>You can set monitoring parameters on the IPS Health Monitor page at [IPS device in Device View] Platform > Device Admin > Health Monitor.</p>
IPS License	<p>Displays IPS devices for which the license will expire in 30 days or 60 days. (Use the dropdown list to choose 30 days or 60 days.)</p> <p>If the license will expire in 30 days or 60 days (whichever you select) this widget displays the license expiry date.</p>
IPS Update Packages	<p>Displays sensor updates and signature updates that are available on Cisco.com or on a local download server but not downloaded to the Security Manager server.</p> <p>If there are many such updates, then this widget displays only the 10 most recent updates.</p>
IPS Sensors Out of Date	<p>Sensors requiring a signature update.</p>
Top 10 Reports for Firewall Sources, Destinations, and Services	<p>Pre-defined system reports that you can use to identify the top destinations, services, and sources for firewall ACL events. The statistics are based on the events collected by the Event Manager service (as displayed in Event Viewer).</p> <p>To use these reports, use Report Manager (Launch > Report Manager...).</p>

Table 71-2 *Description of Individual WidgetsDashboard widgetswidgets for IPS in Dashboardwidgets for firewall in dashboard (Continued)*

Top 10 Reports for Botnet Malware Sites, Ports, and Hosts	<p>Pre-defined system reports that you can use to analyze botnet traffic filtering. The statistics are based on the botnet events collected by the Event Manager service (as displayed in Event Viewer) for blocked and gray-listed sites.</p> <p>To use these reports, use Report Manager (Launch > Report Manager...).</p>
Firewall CPU Usage Trends	<p>A measure of the firewall CPU usage trends. The CPU usage trend data will appear in this widget only when a firewall issues an alert because of CPU usage, and the data will disappear when the alert is cleared.</p>

Table 71-2 *Description of Individual Widgets* **Dashboard widgets for IPS in Dashboard widgets for firewall in dashboard (Continued)**

<p>Device Health Summary</p>	<p>Shows current high- or medium-severity active alerts generated by HPM. Alerts can be grouped by Alert-Description, Predefined-Category, Device, or Alert Technology.</p> <p>Clickable Link—The device name is an active hyperlink; click it to display the Device Summary dialog box in the Dashboard. This link works for any option in the Group by _____ dropdown list: Alert, Category, Device, or Technology.</p> <p>To configure these alerts, use HPM (Launch > Health and Performance Monitor...).</p> <p>Note After enabling a device for monitoring in HPM, it can take up to 5 minutes for priority devices and 10 minutes for non-priority devices before actual values can be seen in the Device Health Summary.</p> <p>Acknowledge Alert—To acknowledge an alert, follow these steps:</p> <ol style="list-style-type: none"> 1. Use the Group by _____ dropdown list to choose Alert, Category, Device, or Technology. 2. Expand the alert, category, device, or technology that you are interested in. Doing this will show you an alert, category, device, or technology for each device that you are monitoring in Security Manager. 3. Click the Details icon (pictured at the end of this topic). Doing this will open the Alert dialog box. 4. Click Acknowledge Alert <p>Clear Alert—To clear an alert, follow these steps:</p> <ol style="list-style-type: none"> 1. Use the Group by _____ dropdown list to choose Alert, Category, Device, or Technology. 2. Expand the alert, category, device, or technology that you are interested in. Doing this will show you an alert, category, device, or technology for each device that you are monitoring in Security Manager. 3. Click the Details icon (pictured at the end of this topic). Doing this will open the Alert dialog box. 4. Click Clear Alert <p>You can also access device health summary information from mobile devices. To do this, use the CSM Mobile application. The information available to you from CSM Mobile is the same as that available in the Device Health Summary widget in the Dashboard. For information on enabling or disabling CSM Mobile, see CSM Mobile Page, page 11-9.</p>
-------------------------------------	--

Table 71-2 Description of Individual Widgets
Dashboard widgets for IPS in Dashboard widgets for firewall in dashboard (Continued)

Memory Usage Trends	<p>A measure of IPS health status or firewall health trends.</p> <p>For IPS devices, you can set monitoring parameters on the IPS Health Monitor page at [IPS device in Device View] Platform > Device Admin > Health Monitor.</p>
Deployment	<p>Shows the deployment status for all devices for the past 24 hours</p> <p>You can also monitor deployment status by using Deployment Manager (Configuration Manager > Manage > Deployments...).</p>
IP Intelligence	<p>Information about an IP address related to the following things:</p> <ul style="list-style-type: none"> • IP Geolocation • FQDN through DNS reverse lookup • WHOIS information <p>For IP Intelligence settings in Security Manager, navigate to Configuration Manager > Tools > Security Manager Administration > IP Intelligence Settings.</p>
CSM Monitor	<p>Shows server information in three categories:</p> <ul style="list-style-type: none"> • CSM Server Statistics. This information is self-explanatory; for example, the operating system boot time is listed. • CSM User Related Information. This information consists of only one item, the number of users logged in. • CSM DB Backup Related Information. This information tells you if the CSM Monitor widget has found a dangling backup lock file. <p>Knowing if you have a dangling backup lock file is important for the following reason: When a CSM backup is performed, it fails with an error similar to this: "Backup failed.ERROR(383): C:\PROGRA~2\CSCOp\backup.LOCK file exists."</p> <p>The solution can be described as follows: Security Manager creates a new lock file (backup.LOCK) in the backup directory before it starts a backup. If a backup is interrupted or fails, the file does not get cleaned up. You must delete the current backup.LOCK file from the Security Manager server, and then execute the backup process again.</p> <p>The CSM Monitor widget makes it faster and more convenient for you to detect a dangling backup lock file.</p> <p>For detailed information, refer to the Cisco TAC document at the following URL: http://www.cisco.com/en/US/products/ps6498/products_tech_not_e09186a0080c13cdd.shtml</p>

**Note**

In some cases, Top Infected Hosts, for example, the dashboard report has a slightly different appearance than the report generated by Report Manager. This is caused by a difference in sorting, but the data is identical. Such a case will occur when more than one entry in the dashboard report has the same count.

Basic dashboard operations are listed in the following table:

Table 71-3 Basic Dashboard Operations

Launch Dashboard	Configuration Manager or other Security Manager client application > Launch > Dashboard...
Add a new dashboard	File > New Dashboard
Re-arrange Dashboard Tabs for a Default View	<p>You can re-arrange the dashboard tabs so that you can set a default view. For example, you might want the IPS tab to be first (on the extreme left):</p> <ol style="list-style-type: none"> 1. Click a tab that you are interested in, e.g., Summary, Firewall, or IPS. 2. While your tab of interest is still selected, right-click to see the following context menu options: Move to Left, Move to Right, Move to First, Move to Last. 3. Click your choice. 4. You do not need to save your changes, and your changes will be persistent--the individual dashboard tabs will be arranged in the same way the next time you launch the Dashboard.
Display a different dashboard	Click the tab for the desired dashboard, such as Summary, Firewall, or IPS.
Show or hide widgets	File > Show Widgets or File > Hide Widgets
Add a widget	<p>Drag-and-Drop Method:</p> <ol style="list-style-type: none"> 1. File > Show Widgets 2. Drag and drop the desired widget onto the dashboard. <p>Menu Method:</p> <ol style="list-style-type: none"> 1. File > Show Widgets 2. Select the desired widget by clicking it. 3. Click Add in the Description bar. 4. Click Done in the Description bar. <p>Note When using the menu method, the widget will be added to the upper left-hand corner of the Dashboard. If desired, you can rearrange all the widgets by dragging and dropping them.</p>
Remove a widget	Click the Remove icon in the title bar of the widget that you want to remove.

Table 71-3 Basic Dashboard Operations*Dashboard operations (Continued)*

Expand a widget	<p>If a widget is shown in the dashboard, you can expand it with the down arrow. The down arrow becomes visible when you hover the mouse pointer over the right side of the widget title bar. The tooltip for the down arrow is labeled "Expand."</p> <p>Note A special consideration applies when you 1) collapse a widget, 2) exit the dashboard, and then 3) launch the dashboard again. In this case, you will find that the widget is still collapsed, but the down arrow (normally used to expand it) is not present; only the up arrow (normally used to collapse it) is present. To expand the widget in this case, click the up arrow, note that the down arrow re-appears, and then click the down arrow as usual.</p>
Collapse a widget	<p>If a widget is shown in the dashboard, you can collapse it with the up arrow. The up arrow becomes visible when you hover the mouse pointer over the right side of the widget title bar. The tooltip for the up arrow is labeled "Expand" (not "Collapse").</p>
Group by _____ (Device Health Summary widget only)	<p>A dropdown list offering you the following choices:</p> <ul style="list-style-type: none"> • Group by Alert • Group by Category • Group by Device • Group by Technology <p>Note In the Group by _____ dropdown list, you can click the display name of a device (underlined to indicate that it is a hyperlink) to see an information box on the health of that device in terms of memory and other parameters. The information box contains an address field; the address can be either Host.Domain or the IP address: if Host.Domain is configured, that information will be displayed; otherwise, the IP address will be displayed.</p>

In the Dashboard, many of the icons can be clicked to accomplish a particular action, such as "Refresh" or "Add Dashboard." Most of these "clickable" icons have a tooltip to document the action that clicking the icon will accomplish, but a few do not. Clickable icons that have no tooltip in the dashboard are documented in the following table.

Table 71-4 Clickable Icons that have no Tooltip in the Dashboard Dashboard icons without tooltips in Dashboard

Icon	Appearance	Widget	Description
	Black exclamation point (bang) on a yellow background in a triangle.	Deployment widget	<p>Deploying icon.</p> <p>Indicates that a job is in the deploying state. Click this icon to open/close the job description:</p> <ul style="list-style-type: none"> • Created date and time • Job Name • Description • State • User • Job Type
	White rectangle (a document) with red and yellow dots.	Deployment widget	<p>Status Report icon.</p> <p>Click this icon to see a detailed Deployment Status report</p>
	White checkmark in a green circle with a grey border.	Deployment widget	<p>Succeeded icon.</p> <p>Indicates that a job is in the success state. Click this icon to open/close the job description:</p> <ul style="list-style-type: none"> • Created date and time • Job Name • Description • State • User • Job Type
	White "X" in a red circle with a grey border.	Deployment widget	<p>Failed icon.</p> <p>Indicates that a job is in the failed state. Click this icon to open/close the job description:</p> <ul style="list-style-type: none"> • Created date and time • Job Name • Description • State • User • Job Type

Table 71-4 *Clickable Icons that have no Tooltip in the Dashboard*
Dashboard icons without tooltips in Dashboard (Continued)

Icon	Appearance	Widget	Description
	Clipboard with a pencil making annotations on a sheet of paper.	Device Health Summary widget	<p>Details icon.</p> <p>Click this icon to open/close the job description:</p> <ul style="list-style-type: none"> • Created date and time • Job Name • Description • State • User • Job Type

CSM Mobile

Beginning with Version 4.5, Cisco Security Manager has an application called CSM Mobile.

CSM Mobile allows you to access device health summary information from mobile devices. The information available to you in this way is the same as that available in the Device Health Summary widget in the Dashboard: current high or medium severity active alerts generated by Health and Performance Monitor. Alerts can be grouped by Alert-Description, Predefined-Category, Device, or Alert Technology. For more details on device health summary information in the Dashboard, see [Dashboard Overview, page 71-1](#).

The principal users of CSM Mobile are expected to be those who use an Apple iPad, an Apple iPhone, the Google Chrome browser, or the Apple Safari browser.

CSM Mobile must be enabled for you to use it. For information on enabling or disabling CSM Mobile, see [CSM Mobile Page, page 11-9](#).



Note

If the CSM Mobile feature is not enabled, you will be redirected to the default Security Manager login page (which is provided by the CiscoWorks Common Services framework software); you will not receive an error message.

The home page for CSM Mobile has the following alert categories:

- Device Not Reachable
- Interface Down
- Overall Device Health Alerts
- High Memory Utilization
- Firewall—High CPU Utilization
- IPS—High Inspection Load
- IPS—High Missed Packets
- IPS—Bypass Mode
- Other Alerts

Navigation and other tasks in CSM Mobile are accomplished by using a few simple screens and icons:

- **Login**—A screen reading "Cisco Security Manager Mobile—Version 4.5.0" with fields for username and password and a button for login.
- **Logout**—On the CSM Mobile home page, a white X icon on a blue background. This icon is located in the upper left-hand corner.
- **Refresh**—On the CSM Mobile home page, a white circular arrow icon on a blue background. This icon is located in the upper right-hand corner.
- **Alert Detail**—For each type of alert on the CSM Mobile Home page, an grey arrow icon to the right of the alert count.
- **CSM Mobile Back Button**—On each alert detail page, a white angle arrow on a blue pentagon-shaped background [available only on alert detail pages]. The CSM Mobile back button is functionally equivalent to your browser's back button.

**Note**

The CSM Mobile display does not refresh itself automatically; you must manually click the refresh button to obtain up-to-date alert data.

Viewing Inventory Status

You can view a summary of device properties for all devices that you are authorized to view. The summary includes device contact information and all device configurations, indicating which settings are local and which are using a shared policy, and indicating any policy object overrides in effect. You can also view the status of configuration deployment to the device.

The report is in table format, allowing you to organize information by filtering, sorting, reordering and removing columns. You can also export the table contents to a comma-separated values (CSV) file on the Security Manager server.

-
- Step 1** In Device view, select **Tools > Inventory Status** to open the [Inventory Status Window, page 71-13](#).
- Step 2** Select the device whose detailed status you want to view in the upper table. The detailed information is shown in the tabs in the lower pane. The information is organized into folders; click the +/- icons to open and close folders, or double-click the folder name. The following tabs are available:
- **Inventory**—Lists summary information about the selected device's device properties, deployment methods, device group membership, and the parent device for modules.
 - **Policy**—Lists the current status of the policies that can be configured for the selected device, whether the policy is unassigned (not defined), a local policy, or a shared policy.
 - **Policy Object Overrides**—Lists policy objects that have overrides defined for the selected device.
 - **Status**—Lists status messages from Security Manager deployment jobs for the selected device, organized by event type.
- An **event** is a notification that a managed device or component has experienced an abnormal condition. Multiple events can occur simultaneously on a single monitored device or service module.
- Security Manager displays only the most-recent event of each type. To view historical status information, use the Deployment Manager.
- Step 3** Click **Close** to close the Inventory Status window.
-

Inventory Status Window

Use the Inventory Status window to view device properties and status for the devices that you are allowed to view. This window summarizes device information so that you do not have to open the device properties for each individual device.

In addition to device property information, you can view summary information about how the policies on each device are configured (whether local, shared, or not configured) and the policy objects that have overrides for each device. You can also view the status of configuration deployment to the device.

The Inventory Status window contains two panes. Use the upper pane to view a complete listing of all devices, to sort the devices by attribute, or to filter out certain ones. Use the lower pane to view the device property details of the device selected in the upper pane.

Navigation Path

Select **Tools > Inventory Status**.

Related Topics

- [Viewing Inventory Status, page 71-12](#)
- [Filtering Tables, page 1-48](#)
- [Table Columns and Column Heading Features, page 1-49](#)

Field Reference

Table 71-5 *Inventory Status Window*

Element	Description
Device Summary Information for All Devices (Upper Pane)	
Export button	Click this button to export the inventory as a comma-separated values (CSV) file. You are prompted to specify a file name and to select a folder on the Security Manager server. You can use the export file for reference or analysis.
Display Name	The name of the device as it is displayed in Security Manager.
Deployment	The status of the configuration deployment for the device.
OS Type	The family of the operating system running on the device, for example, IOS, IPS, ASA, FWSM, or PIX.
Running OS Version	The version of the operating system running on the device.
Target OS Version	The target OS version for which you want to apply the configuration. Configurations are based on the commands supported by this version.
Host Name.Domain Name	The DNS host and domain names for the device.
IP Address	The management IP address of the device.
Device Type	The type of device.

Details for the Selected Device (Lower Pane)

The detailed information is shown in the tabs in the lower pane. The information is organized into folders; click the +/- icons to open and close folders, or double-click the folder name.

Table 71-5 *Inventory Status Window (Continued)*

Element	Description
Inventory	Lists summary information about the selected device's device properties, deployment methods, device group membership, and the parent device for modules.
Policy	Lists the current status of the policies that can be configured for the selected device, whether the policy is unassigned (not defined), a local policy, or a shared policy.
Policy Object Overrides	Lists policy objects that have overrides defined for the selected device. For more information on policy object overrides, see Policy Object Override Pages, page 3-51 .
Status	Lists any deployment status messages for the selected device. Events are organized by event type. Event details include timestamp, description, and recommended action. The time stamp indicates the time of the last change in status for the device, not the time of the latest polling of the device. Also shown is the highest severity level of the status messages.
Navigation buttons	Click the navigation buttons to move through the inventory list. From left to right, buttons mean go to the first device in the list, go to the previous device, go to the next device, and go to the last device. The center field indicates which device is currently selected based on the row number (for example 5/10 means the fifth of 10 devices in the list).

Starting Device Managers

You can start a device manager to view a device's configuration and status from within Security Manager. You can start device managers for ASA, ASA-SM, PIX, FWSM, IPS, and IOS devices. Each device manager includes several monitoring and diagnostic features that provide information regarding the services running on the device and a snapshot of the overall health of the system. You can use these device managers to view the existing device configuration and to monitor current status, but you cannot use it to apply configuration changes to the device.



Note

You cannot start device managers for IPS virtual sensors.

To start a device manager, select the device in Device view, right-click and select **Device Manager**. You can also start the device manager by selecting **Launch > Device Manager**. (These commands are disabled when you select an ASA CX device, and the **Prime Security Manager** commands are enabled. Cisco Prime Security Manager is used to configure and manage ASA CX devices. See [Launching Cisco Prime Security Manager or FireSIGHT Management Center, page 71-20](#) for more information.)

When you start a device manager from Security Manager, the device manager executable is downloaded to your client system; the device manager does not need to be installed on the network device. The first time you start a device manager, it takes time to download the software to your workstation (you are shown a progress bar). (If you run into problems, review the tips in [Troubleshooting Device Managers, page 71-16](#).)

Security Manager selects the most appropriate device manager version based on the operating system running on the network device. Subsequent communications with the selected device are completely transparent. Connections are made through the Security Manager server; that is, the Security Manager server acts as a proxy server. By starting a device manager from Security Manager, you eliminate the need to open an HTTPS connection between your client system and the device you want to monitor.

**Tip**

When you start a device manager session, Security Manager opens a version of the manager that is appropriate for the operating system software version running on the device. However, Security Manager might not open the most recently-available version of the device manager if new device manager versions have been released after the release of the Security Manager version you are using. When you start the device manager, check its version (for example, select **Help > About** in the device manager window); if there is a more recent device manager available with features that you require, you must install and use that device manager outside of Security Manager to use those new features.

Keep in mind that if you use an external device manager running on the device to modify device configurations directly, these changes are considered out-of-band by Security Manager, and might be subsequently overwritten when you next deploy configurations from Security Manager. For more information about out-of-band changes, and what you can do to identify and recreate them, see the following topics:

- [Understanding How Out-of-Band Changes are Handled, page 8-12](#)
- [Detecting and Analyzing Out of Band Changes, page 8-45](#)

Security Manager starts only one instance of a device manager per device, and closes the device manager when you exit Security Manager, or when the idle-session timeout period is exceeded. You can have more than one device manager window open at one time (connected to different devices).

The following table outlines the device managers you can launch from Security Manager.

Table 71-6 **Device Managers Available in Security Manager**

Device Manager	Description
IDM	The IPS Device Manager (IDM) lets you monitor IPS sensors and modules that are part of the Security Manager inventory. See the IDM documentation for more information about using this device manager.
PDM	The PIX Device Manager (PDM) lets you monitor PIX 6.x devices and early FWSMs, specifically FWSM releases 1.1, 2.2 and 2.3 in single- or multiple-context modes. See the PDM documentation for more information about using this device manager.
ASDM	The Adaptive Security Device Manager (ASDM) lets you monitor ASA, ASA-SM, PIX 7.x+, and FWSM 3.x+ devices. See the ASDM documentation for more information about using this device manager.

Table 71-6 Device Managers Available in Security Manager (Continued)

Device Manager	Description
SDM	The Security Device Manager (SDM) lets you monitor Cisco IOS-based resources. SDM requires no previous experience with Cisco devices or the Cisco command-line interface (CLI). Cisco SDM supports a wide range of Cisco IOS software releases. See the SDM documentation for more information about using this device manager.

The following topics explain more about troubleshooting and using device managers:

- [Troubleshooting Device Managers, page 71-16](#)
- [Access Rule Look-up from Device Managers, page 71-17](#)
- [Navigating to an Access Rule from ASDM, page 71-18](#)
- [Navigating to an Access Rule from SDM, page 71-19](#)

Troubleshooting Device Managers

If you can successfully deploy configurations to a device, Security Manager should be able to open a device manager session with the device (as described in [Starting Device Managers, page 71-14](#)). However, if you have problems making a connection or using one that is open, consider the following troubleshooting tips, which are divided into basic tips and tips for using multiple device managers.

Basic Device Manager Troubleshooting Tips

- Generally, the credentials configured for the device in the Security Manager inventory are used to start the device manager. However, some versions of SDM require that you enter a user name and password when the device manager is started. If you get an error that says device credentials are missing, or they are not valid, update the Device Properties Credentials page with a username and password that can log into the device. In Device view, right-click the device and select **Device Properties**. For more information, see [Viewing or Changing Device Properties, page 3-40](#) and [Device Credentials Page, page 3-45](#).
- All users associated with any of the CiscoWorks Common Services roles have permission to start device managers from Security Manager, with the exception of the Help Desk role or any of the predefined Cisco Secure ACS roles. Ensure you have appropriate permissions.
- SSL/HTTPS must be enabled on the target device to provide secure communications between Security Manager and the device. An error message is displayed if SSL is not enabled on the device. See [Understanding Device Communication Requirements, page 2-1](#) for more information.
- You might need to modify Cisco Security Agent, or other anti-virus and network firewall software, on the Security Manager system and on your workstation to allow the device manager service (`xdm-launcher.exe`) to be started.
- Ensure that Security Manager is correctly configured for contacting and communicating with the target device. Specifically verify device properties such as identity, operating system and credentials. Select the desired device, right-click and choose **Device Properties**. Verify the settings on the General and Credentials pages. You can test whether Security Manager can connect to the device by selecting the Credentials tab and clicking **Test Connectivity** (see [Testing Device Connectivity, page 9-1](#)).

- Device managers can be started for FWSMs and ASAs running in transparent mode (Layer 2 firewall) or routed mode (Layer 3 firewall), and supporting a single security context or multiple security contexts. For FWSM and ASA devices running multiple security contexts, you must define a unique management IP address for each security context.
- If you get a message saying that the platform is not supported for device manager launch, but you believe the platform should be supported based on information in this guide, consider the relative newness of the operating system version running on the device and the age of the Security Manager software version you are using. If you are using very recent operating systems, but a relatively older version of Security Manager, you might need to upgrade Security Manager (or apply a service pack), contact Cisco Technical Support, or simply install the latest device manager on the network device and use it outside of Security Manager. Before using a device manager outside of Security Manager, review the information on out-of-band changes in [Starting Device Managers, page 71-14](#).

Multiple Device Manager Sessions Troubleshooting Tips

- Starting multiple device managers might affect the performance of both the Security Manager server and your client. On the client, memory requirements and performance impact are proportional to the number of device managers launched. On the server, a large number of requests to start device managers or retrieve current information from the device can have an adverse impact on performance.
- The maximum number of persistent HTTPS connections that can be established with any one device from all clients depends on the device type and model. An error message is displayed if you attempt to exceed this limit.

For example, a single PIX 6.x allows multiple clients to each have one browser session open, supporting up to 16 concurrent PDM sessions. An FWSM (1.1, 2.2, or 2.3) allows up to 32 PDM sessions for the entire module, with a maximum of five concurrent HTTPS connections per context.

Refer to the appropriate device documentation for information about specific limits.

Access Rule Look-up from Device Managers

A set of access rules is associated with each device interface. These rules are presented in the form of an ordered list or table. This list is often referred to as an access-control list (ACL), with each rule in the list known as an access-control entry (ACE). When deciding whether to forward or drop a packet, the device tests the packet against each access rule in the order listed. When a rule is matched, the device performs the specified action, either permitting the packet into the device for further processing, or denying entry. If the packet does not match any rule, the packet is denied.

Activity on your firewall or router can be monitored through syslog messages. If logging is enabled on the device, whenever an access rule that is configured to generate syslog messages is matched—for example, a connection was attempted from a denied IP address—a log entry is generated.



Note

For the device to generate log entries, logging must be enabled on the device (on the [Logging Setup Page](#) for ASA/PIX devices and the Logging policies for IOS devices, described in [Logging on Cisco IOS Routers, page 64-1](#)), and the individual access rules must be configured to generate log messages when they are matched (in the [Advanced and Edit Options Dialog Boxes, page 16-17](#)).

You can monitor syslog messages in device managers launched from Security Manager. For certain device managers, you can also look up the access rule in Security Manager that generated a particular message from the monitoring window. The access rule that triggered the syslog entry is highlighted in Security Manager on a first-match basis, even if there are multiple matches.

This access rule look-up is available through SDM for all managed routers running IOS, and through ASDM for managed PIX and ASA devices (including ASA-SM) running version 8.0(3) and above, and FWSM devices running version 3.1 and above.

The following topics describe how to look up access rules in Security Manager from a device manager:

- [Navigating to an Access Rule from ASDM, page 71-18](#)
- [Navigating to an Access Rule from SDM, page 71-19](#)

Navigating to an Access Rule from ASDM

In an ASDM device manager launched from Security Manager, you can monitor system log messages in the Real-time Log Viewer window and the Log Buffer window. You can select a syslog message displayed in either window and navigate to the access-control rule in Security Manager that triggered the message, where you can update the rule as necessary.

The Real-time Log Viewer is a separate window that lets you view syslog messages as they are logged. The separate Log Buffer window lets you view messages present in the syslog buffer.

You can look up access rules associated with the following syslog message IDs:

- 106023 – Generated when an IP packet is denied by the access rule. This message appears even when logging is not enabled for the rule.
- 106100 – If logging is enabled for a matched access rule (in the [Advanced and Edit Options Dialog Boxes, page 16-17](#)), this message provides information about the traffic flow, depending on the parameters set. This message provides more information than message 106023, which logs only denied packets.

This procedure describes how to look up an access rule in Security Manager from ASDM's Real-time Log Viewer or Log Buffer windows.

Related Topics

- [Access Rule Look-up from Device Managers, page 71-17](#)
- [Navigating to an Access Rule from SDM, page 71-19](#)

-
- Step 1** Select a PIX, ASA, ASA-SM, or FWSM in the Security Manager device inventory.
- Step 2** Select **Launch > Device Manager** to start ASDM. For more information about starting device managers, see [Starting Device Managers, page 71-14](#).
- Step 3** In the ASDM window, click the **Monitoring** button to display the Monitoring panel; click **Logging** in the left pane to access the log-viewing options.
- Step 4** Select either **Real-time Log Viewer** or **Log Buffer**.
- Step 5** Click the **View** button to open the selected log-viewing window.



Note The View button is not displayed if logging is not enabled on the device.

Each syslog message listed in the window includes the following information: message ID number, date and time the message was generated, the logging level, and the network or host addresses from which the packet was sent and received.

- Step 6** To view the access rule that triggered a specific syslog message, select the message and click the **Show Rule** button in the ASDM toolbar (or right-click the message and choose **Go to Rule in CSM** from the pop-up menu).

The Security Manager client window is activated and the Access Rules page appears with the rule highlighted in the rules table. If the syslog entry was triggered by an access rule not referenced in the current Security Manager activity, an error message appears.

Navigating to an Access Rule from SDM

In an SDM device manager launched from Security Manager, you can view a log of events categorized by security level under the Syslog tab of the Logging window. You can select a syslog message and navigate to the access-control rule in Security Manager that triggered the message, where you can update the rule as necessary.

The Monitor > Logging option in SDM offers four log tabs; Syslog is the only one of these offering the Security Manager access-rule look-up option. The router contains a log of events categorized by severity level. The Syslog tab displays the router log, even if log messages are being forwarded to a syslog server.

On Cisco IOS devices, syslog messages are generated for access rules configured with the **log** or **log-input** keywords. The **log** keyword produces a message when a packet matches the rule. The **log-input** keyword produces a message that includes ingress interface and source MAC address, in addition to the packet's source and destination IP addresses and ports. When identical packets are matched, the message is updated at five-minute intervals with the number of packets permitted or denied in the previous five minutes.

This procedure describes how to look up an access rule in Security Manager from the Syslog tab of SDM's Logging panel.

Related Topics

- [Access Rule Look-up from Device Managers, page 71-17](#)
- [Navigating to an Access Rule from ASDM, page 71-18](#)

-
- Step 1** Select an IOS router in the Security Manager device inventory.
- Step 2** Select **Launch > Device Manager** to start SDM. For more information about starting device managers, see [Starting Device Managers, page 71-14](#).
- Step 3** In the SDM window, click the **Monitoring** button to display the Monitoring panel; click **Logging** in the left pane to access the log-viewing options.
- The Logging pane appears with Syslog tab displayed.
- Step 4** To view the access rule that triggered a specific syslog message, select the message and click the **Go to Rule in CSM** button above the table of log messages.

The Security Manager client window is activated and the Access Rules page appears with the rule highlighted in the rules table. If the syslog entry was triggered by an access rule not referenced in the current Security Manager activity, an error message appears.

Launching Cisco Prime Security Manager or FireSIGHT Management Center

The ASA CX is an Adaptive Security Appliance module that provides advanced ConteXt-aware security, extending the ASA platform to provide in-depth “who-what-where-when-how” application visibility and control. The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

The ASA CX devices are managed by the Cisco Prime Security Manager (PRSM) application and the ASA FirePOWER modules are managed by the FireSIGHT Management Center application—they cannot be directly managed by Cisco Security Manager. However, Security Manager has been enhanced to allow you to discover the presence of these modules on ASA devices; to “cross launch” PRSM and FireSIGHT Management Center from the Configuration Manager application; and to share Policy Object data between Security Manager and PRSM.



Note

PRSM and FireSIGHT Management Center are browser-based applications; that is, they are launched and operate within a browser window. Therefore, when you cross-launch PRSM or FireSIGHT Management Center from the Configuration Manager client, the host system’s default browser is opened and the management application initiated. However, some browsers have not been certified with PRSM or FireSIGHT Management Center and you may need to change the default browser on the Security Manager client’s host system prior to cross-launching. See “Browser Requirements” in the PRSM or FireSIGHT Management Center installation guide for more information.

Before You Begin

In order to cross-launch PRSM or FireSIGHT Management Center, Security Manager must be aware of the presence of the modules. This is accomplished through discovery of either new ASA devices, or of modules which have been added to existing ASAs. This process is outlined in [Detecting ASA CX and FirePOWER Modules](#), page 71-21.

Also, you can enable and configure “single sign-on” (SSO) to allow Security Manager users direct access to PRSM or FireSIGHT Management Center without logging into the applications separately. To allow this, the appropriate user credentials must be defined in both applications. (Note that SSO is not necessary to cross-launch PRSM or FireSIGHT Management Center.) See Security Manager’s [Single Sign-on Configuration Page](#), page 11-67, and “Configuring Single Sign-On for Cisco Security Manager” in the *User Guide for ASA CX and Cisco Prime Security Manager* ([Cisco ASA CX Context-Aware Security End-User Guides](#)) for more information.

Related Topics

- [Single Sign-on Configuration Page](#), page 11-67
- [Detecting ASA CX and FirePOWER Modules](#), page 71-21
- [Sharing Device Inventory and Policy Objects with PRSM](#), page 71-22

To monitor and manage your ASA CX devices or FirePOWER Modules, cross-launch PRSM or FireSIGHT Management Center:

-
- Step 1** Select a previously discovered ASA CX device or ASA with FirePOWER module in Configuration Manager’s Device view—in either the device-selector tree, or the table of devices in the content area. Again, discovering ASA CX devices or FirePOWER modules in Security Manager is described in [Detecting ASA CX and FirePOWER Modules](#), page 71-21.

- Step 2** Right-click the selected device and choose **Prime Security Manager** or **FireSIGHT Management Center** from the pop-up menu. Alternatively, you can choose **Prime Security Manager** or **FireSIGHT Management Center** from the Configuration Manager's **Launch** menu. (These commands are available only when you have selected an ASA CX or an ASA with a FirePOWER module.)

The browser-based PRSM or FireSIGHT Management Center window appears, displaying the device screen for the selected device.



Note The URL used by Security Manager to launch PRSM incorporates the management IP address of the CX module (obtained during device detection), and includes the string `/admin/mgmt?rtp`. During cross-launch, this type of request is redirected to the appropriate PRSM central server, if one exists. Otherwise, the “on-box” version of PRSM is launched. (To directly launch the on-box version of PRSM yourself, you must type `https://<management_IP_address>`, where `<management_IP_address>` is the management address of the desired CX module, into your browser's address field.)

Information about using PRSM can be found on the [Cisco ASA CX Context-Aware Security End-User Guides](#) page of cisco.com and information about using FireSIGHT Management Center can be found on the [Cisco FireSIGHT Management Center](#) page of cisco.com.

Detecting ASA CX and FirePOWER Modules

Prior to being able to share Policy Object data between Security Manager and PRSM, and to cross-launch PRSM or FireSIGHT Management Center from Configuration Manager, you must ensure that Security Manager is aware of the module.

Detection of a CX or FirePOWER module is automatic when you discover a new ASA device by selecting the relevant options in the New Device wizard, as described in [Adding Devices to the Device Inventory, page 3-7](#).

When you add a CX or FirePOWER module to an ASA device already in the inventory, you can detect the new module without affecting the existing policies on the host ASA, as follows:

1. Select one or more ASA devices in Configuration Manager's device-selector tree.
You can detect more than one module at once—any selected devices that are not ASAs, or that are ASAs which do not include a CX or FirePOWER module, are ignored.
2. Right-click any selected device and choose **Detect ASA-CX/FirePOWER Module** from the pop-up menu.

The Create Discovery Task dialog box or Bulk Rediscovery dialog box appears, with the *Detect ASA-CX/FirePOWER Module* option selected—none of the other discovery options are available.

See [Create Discovery Task and Bulk Rediscovery Dialog Boxes, page 5-18](#) for more information about using this dialog box.

3. Click **OK** on the Create Discovery Task dialog box or click **Finish** on the Bulk Rediscovery dialog box to close the dialog box and begin module detection.

You may be warned that discovery will replace existing policies; you can safely click Yes to close the warning and proceed.

The Discovery Status dialog box opens automatically displaying discovery progress; see [Viewing Policy Discovery Task Status, page 5-22](#) for more information about this process.

When a CX or FirePOWER module is detected on an ASA, the management IP address of the module itself is fetched and the ASA-CX/FirePOWER Module section of the Device Properties window is updated; see [Device Properties: General Page, page 3-41](#). The management IP address is used to cross-launch PRSM or FireSIGHT Management Center. (Cisco Prime Security Manager, or PRSM, is the application used to configure and manage ASA CX devices and FireSIGHT Management Center is the application used to configure and manage ASA FirePOWER modules, as described in [Launching Cisco Prime Security Manager or FireSIGHT Management Center, page 71-20](#).)

**Note**

The URL used by Security Manager to launch PRSM incorporates the management IP address of the CX module (obtained during device detection), and includes the string `/admin/mgmt?rtp`. During cross-launch, this type of request is redirected to the appropriate PRSM central server, if one exists. Otherwise, the “on-box” version of PRSM is launched. (To directly launch the on-box version of PRSM yourself, you must type `https://<management_IP_address>`, where `<management_IP_address>` is the management address of the desired CX module, into your browser’s address field.)

Upon completion of the detection process, all ASAs with CX modules installed are indicated in the various Security Manager displays by presentation or inclusion of the PRSM icon: . For example, here is the ASA CX icon used in the Device selector: .

**Caution**

You also can detect the presence of a CX or FirePOWER module on an existing ASA by choosing **Discover Policies on Device(s)** from the selected-device right-click menu, or by choosing **Discover Policies on Device** from the Policy menu. Depending on the number of devices selected and which command you choose, the Create Discovery Task dialog box, or the Bulk Rediscovery Task dialog box, opens and all discovery-rediscovery options are available. This means you can potentially overwrite any shared policies already established on the selected device(s). Be sure to deselect all options except **Detect ASA-CX/FirePOWER Module**, unless you are sure you want to rediscover existing policies. See [Discovering Policies on Devices Already in Security Manager, page 5-15](#) for more information.

Sharing Device Inventory and Policy Objects with PRSM

You can export the current device inventory, and the current set of policy objects, as defined in Security Manager for import into Cisco Prime Security Manager (PRSM).

Exporting the Device Inventory

To share the Security Manager device inventory with PRSM, export the inventory as a comma-separated values (CSV) file, as described in [Exporting the Device Inventory, page 10-6](#). Be sure to specify “Cisco Security Manager” as the format type for the export file.

Exporting Networks/Hosts and Services Policy Objects

To export Security Manager policy objects—specifically Networks/Hosts objects, or Services objects; PRSM does not support Port List objects—for import into PRSM, you must execute a Perl script on the Security Manager server host to create a CSV file.

The Perl script is included in the Security Manager server installation, and its use is described in detail in [Importing and Exporting Policy Objects, page 6-23](#). The basic procedure is as follows:

1. Log into the computer running the Security Manager server, open a Cmd window, navigate to the Perl-script location, and then execute the Perl-script command at the command prompt.

Here is an example of the command as used to export Networks/Hosts objects: `perl PolicyObjectImportExport.pl -u user -p password -o export -t network -f C:\CSM_Net_objects.csv -e true`

2. Copy the CSV file to the PRSM client system.
This file can be edited, if necessary.
3. Launch PRSM and import the CSV file. For information about this process, see the section “Importing Objects” in the “Managing Policy Objects” chapter of the PRSM user guide.

Analyzing an ASA or PIX Configuration Using Packet Tracer

Packet tracer is a policy debugging tool for ASA and PIX security appliances running version 7.2.1+ that are operating in router mode.

The packet tracer inspects the active policies currently running on the appliance. Without having to generate real traffic, you can analyze how traffic between two addresses traverses the security appliance, whether it is dropped or allowed. If the result is unexpected, you can determine where the issue exists and update the corresponding policy in Security Manager to resolve it.

Packet tracer presents a step-by-step analysis of how a simulated packet is processed by the security appliance’s active configuration. It traces the packet’s flow through the active firewall modules, such as route lookup, access lists, NAT translations, and VPN. The set of active modules changes based on the type of packet configured and the active configuration. For example, if no VPN policies are configured, the VPN module is not evaluated.

You can inspect the simulated packet’s traversal rather than having to generate network traffic, enable syslog messages, and manually review resulting syslog messages. Packet tracer details the actions enforced by the active configuration on the packet. If a configuration command causes the packet to be dropped, the reason is provided, such as “Drop-reason: (telnet-not-permitted) Telnet not permitted on least secure interface.”

You can trace the life span of a simulated packet through the security appliance to see whether the packet is behaving as expected. Packet tracer uses include the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet including the CLI that defines the rule.
- Show a time line of packet changes in a data path.
- Trace packets in the data path.
- If the packet is blocked or permitted by some explicit access rule, you can use a short-cut to go to the policy so that you can edit the rule.

Tips:

- Packet Tracer is also available in the ASDM application and the ASA command line, and the Security Manager version is equivalent to the ASDM version. For an example of using Packet Tracer from ASDM and the CLI to analyze a configuration, see [PIX/ASA 7.2\(1\) and later: Intra-Interface Communications](#).
- Before you can use packet tracer on a device, you must submit your policy changes at least once after adding the device to the inventory.

- Packet tracer analyzes only the active configuration running on a device. Therefore, you cannot use packet tracer to test proposed configurations before they are deployed and running on the device. Do not use packet tracer on a device with pending configuration changes—deploy the changes first and then use packet tracer to ensure the packet tracer results are valid.

To use Packet Tracer:

-
- Step 1** (Device view) Right click on the ASA or PIX 7.2.1+ device and select **Packet Tracer** on the shortcut menu to open the Packet Tracer window.
- Step 2** Select the interface you want to test from the **Interfaces** list. The list contains all interfaces defined on the device.
- Step 3** Model the packet that you want to trace by configuring the following fields:
- **Packet Type**—Select whether you are tracing a TCP, UDP, ICMP, or IP packet.
 - **Source, Destination IP Address**—Select from the following address types and enter the host addresses for both ends of the communication (from source to destination):
 - IP Address of the host. This can be IPv4 or IPv6 addresses. Packet tracer with IPv6 is not supported for devices running ASA software version lower than 8.4(2).
 - User (source only). For example, DOMAIN\Administrator. The IP address mapped to the user is used for the trace. You must enable identity-aware firewall by configuring identity options to use this type of address.
 - FQDN, or fully-qualified domain name, of the host. For example, host.example.com. You must configure DNS to use this type of address.
 - Security Name (ASA 9.x+ only).
 - Security Tag (ASA 9.x+ only).
 - **Source, Destination Port (TCP and UDP only)**—Enter, or select, the port numbers that represent the traffic type. The selection list uses names that equate to the standard port numbers for the named application. For example, selecting **http** and entering **80** is the same.
 - **Type, Code, ID (ICMP only)**—When modeling an ICMP packet, you must enter values in all of these fields:
 - **Type**—Select the ICMP packet type or enter the equivalent number. The list includes all main ICMP types. For a complete list of types and related codes, see RFC 1700 at <http://www.ietf.org/rfc/rfc1700.txt> and search for “ICMP Type Numbers.”
 - **Code**—Enter **0** unless you are modeling a packet type that has non-zero codes. These are destination unreachable (type 3, codes 0-12), redirect (type 5, codes 0-3), time exceeded (type 11, codes 0-1), and parameter problem (type 12, codes 0-2). See RFC 1700 for code explanations, and note that additional codes might have been introduced in other RFCs.
 - **ID**—You must enter a value for ID even though the field is used for a limited number of message types only. The ID is used for ICMP types that include request and reply versions, such as echo and echo request, to help match replies to requests. The value should be between 1-255.
 - **Protocol (IP only)**—Enter the number that identifies the next level protocol. For a complete list of protocol codes, see RFC 1700 at <http://www.ietf.org/rfc/rfc1700.txt> and search for the “Protocol Numbers” heading. As of the writing of this topic, numbers 1-54 and 61-100 represent values assigned to actual protocols from the accepted range of 0-255.
 - **VLAN ID (1- 4096)**—Enter the VLAN ID for the flow. The VLAN ID determines, which VLAN the packet belongs to. Cisco Security Manager validates the ID range to be between 1 and 4096.



Note Beginning with Version 4.13, Cisco Security Manager Packet tracer supports the transparent FW devices. Vlan ID is the new parameters introduced in Version 4.13 to support the packet tracer on devices 9.7.1 onwards.

- **Destination MAC**—Enter the destination MAC address for the flow. Cisco Security Manager validates the MAC address for its format.

Step 4 If you want to see the progress of the trace while it is happening, select **Show animation**. Otherwise, the window is not updated with the results until the trace is completed.

Step 5 Click **Start** to trace the packet.

The policies are examined, and the bottom of the window shows the results in two forms: graphical and detailed information. The graphical view summarizes the phases evaluated in the packet's path. Checkmarks indicate the packet passed the phase, a red X indicates the packet was dropped at that point.

The detailed information organizes the results in folders that correspond to the phases, with an Action column that indicates the results of the phase (checkmark for passed, red X for dropped). To open a folder, click its heading. Detailed information can include the specific configuration commands evaluated and the data derived from **show** commands. The final folder, named Result, summarizes the results of the trace.

Tips:

- If the packet is allowed or denied by an explicit access rule, then you can jump to that rule. Select the Access-List folder to open it, then click the **Show access rule** link at the top of the section. You are taken to the Access Rule policy with the rule highlighted; you can edit the rule as desired. If a packet is dropped due to an implicit drop rule, the Show access rule link is not available because the rule does not exist in the policy table.
- If the device is shut down or not reachable due to a network failure during the analysis, an error message stating "Device Connectivity is Failed" appears.
- If you start a new trace, the information shown is cleared automatically. However, you can clear it yourself by clicking **Clear**.

Analyzing Connectivity Issues Using the Ping, Trace Route, or NS Lookup Tools

You can use the Ping or Trace Route tools to investigate and troubleshoot your network configuration and connectivity. You typically run these commands in the device, from within Security Manager by specifying specific launch points and parameters. This causes Security Manager to generate the corresponding command. NS Lookup, on the other hand, is typically run from the Security Manager client.



Note Beginning with Version 4.13, Cisco Security Manager trace routes supports IPv6 address. From ASA version 9.7.1, traceroute for IPv6 address is supported.

Table 71-7 Profiles of the Ping, Trace Route, and NS Lookup Troubleshooting Commands

Tool	Profile
Ping	Use Ping to test whether a particular host is reachable across an IP network and to measure the round-trip time for packets sent from the local host to a destination computer. This can include measuring the local host's own interfaces using ICMP messages. See Analyzing Configuration Using Ping, page 71-26 for details on using this tool.
Trace Route	Use trace route to show the route taken by packets across an IP network. The system returns the number of hops taken and the addresses of each device traversed. See Analyzing Configuration Using TraceRoute, page 71-28 for details on using this tool.
NS Lookup	Use NS lookup (namespace lookup) to issue an NS lookup command from a device so you can test the contents of the DNS server that the queried device uses. See Analyzing Configuration Using NS Lookup, page 71-29 for details on using this tool.

Applicability

The Ping tool is applicable on the following devices: ASA (7.0 – 8.3), PIX [6.3(1-5) to 8.0(2-4)], FWSM [2.2(1) – 4.1(1)], all IOS. It is not applicable to IPS.

The Trace Route tool is applicable on the following devices: ASA [7.2(1) and onward], PIX [6.3(1-5) to 8.0(2-4)], and all IOS. It is not applicable to FWSM nor IPS.

The NS Lookup tool is not supported in any of the devices managed by Cisco Security Manager; rather, you run it from the Cisco Security Manager client using the Windows API.

Analyzing Configuration Using Ping

The ping tool, by default uses the ICMP echo request and echo reply messages to test reachability to a remote system. You can also choose to employ TCP to ping. In its simplest form, ping simply confirms that an IP packet is capable of getting to and getting back from a destination IP address. A ping is sent to an IP address and it returns a reply. This process enables network devices to discover, identify, and test each other. From within Security Manager, you can designate both the network device from which to issue the ping command, and the target of the echo request. This tool generally returns two pieces of information: whether the source can reach the destination (and, by inference, vice versa), and the round-trip time (RTT, typically in milliseconds).

You can use the Ping diagnostic tool in a variety of ways, including:

- **Pinging to a security appliance**—Ping an interface on another security appliance to verify that it is up and responding.
- **Loopback testing of two interfaces**—Initiate a ping from one interface to another on the same security appliance, as an external loopback test to verify basic “up” status and operation of each interface.

- **Pinging through a security appliance**—Ping packets originating from the Ping tool may pass through an intermediate security appliance on their way to a device. The echo packets also pass through two of its interfaces as they return. You can use this to perform a basic test of the interfaces, operation, and response time of the intermediate unit.
- **Pinging to test intermediate communications**—Initiate a ping from a security appliance interface to a network device that is known to be functioning correctly and returning echo requests. If you receive the echo, you confirm physical connectivity and the correct operation of any intermediate devices.

**Tip**

From within the Event Manager, you can right-click on an event to open the Ping Tool and ping the associated device.

Step 1 In Device view, select **Tools > Ping, TraceRoute and NS Lookup . . .**

The Ping, TraceRoute and NS Lookup dialog box appears.

Step 2 From the device selector, select the device from which to issue the **Ping** command.

The selected device is listed in the top right of the dialog box.

**Note**

To employ TCP for the ping, select TCP for the Packet Type. (The default packet type is ICMP)

Step 3 In Hostname/IPv4address, enter the IP address of the host network/host policy object to be pinged.

Alternatively, click **Select** to choose a host network/host object that defines the host network/host policy object to be pinged.

Step 4 Enter a timeout value. [Optional]

Step 5 Click **Ping**.

The results are displayed in the lower window area.

Example Ping output:

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Example Ping unsuccessful output:

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
```

```
?????
```

```
Success rate is 0 percent (0/5)
```

You can click **Clear Output** to remove the previous response from the Ping output area.

For additional details on the **ping** command, see [Troubleshooting TCP/IP](#) on Cisco.com.

Analyzing Configuration Using TraceRoute

The Traceroute tool helps you to determine the route that packets will take to their destination. The tool prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. Traceroute can return useful information about TCP/IP connectivity across your network. The following table shows some of the codes that can be returned by the Traceroute utility, along with their possible cause.

Table 71-8 Traceroute Output Symbols

Output Symbol	Description
*	No response was received for the probe within the timeout period.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable.
!H	ICMP host unreachable.
!P	ICMP unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Step 1 In Device view, select **Tools > Ping, TraceRoute and NS Lookup . . .**

The Ping, TraceRoute and NS Lookup dialog box appears.



Tip From within the Event Manager, you can right-click on an event to open the TraceRoute page and trace the route of the associated device.

Step 2 Select the **Trace Route** tab.

The Trace Route page appears.

Step 3 From the device selector, select the host from which the route is traced.

Step 4 Enter the **IP Address/Hostname** to specify the address or name of the host to which the route is traced. Alternatively, click **Select** to choose a host network/host object that defines the IP address.



Note Beginning with Version 4.13, Cisco Security Manager trace routes supports IPv6 address. Till Version 4.12, the Syslog server was configured with Devices having IPv4 address. From Device version 9.7.1, traceroute for IPv6 address is supported. The Syslog server can be configured with IPv6 syslog address with devices having IPv6 addresses.

Step 5 Specify values, as required, for the following:

Table 71-9 Traceroute Fields

Field	Description
Timeout [optional]	The amount of time, in seconds, to wait for a response before the connection times out. The default is three seconds.

Table 71-9 Traceroute Fields (Continued)

Field	Description
Port [optional]	The destination port used by the UDP probe messages. The default is 33434.
Probes per hop [optional]	The number of probes to be sent at each TTL level. The default is three.
TTL Min [optional]	The minimum TTL value for the first probes. (Default is 1.)
TTL Max [optional]	The maximum TTL value for the first probes.(Default is 30.)

Step 6 If desired, select **Specify Source Interface or IP Address**, and then do one of the following:

- Select a source **Interface** from the drop-down list



Note If an IPv6 address is specified in the **IP Address/ Hostname** field, the source **Interface** field is not applicable.

- Enter an **IP Address**

Step 7 If desired, select **Reverse Resolve** to reverse between displaying the address or hostname.

Step 8 If desired, select **ICMP** to use that protocol rather than IP.

Step 9 Click **Trace**.

The traceroute terminates when the packet reaches the destination or when the TTL Max value is reached. The hops taken and the device address corresponding to each hop are displayed.

Analyzing Configuration Using NS Lookup

You use the NS Lookup tool to look up a remote host address when you have the hostname, or to look up the hostname when you have the address.

Unlike the Ping and Traceroute tools, NS Lookup is done on the Security Manager client.

Step 1 In Device view, select **Tools > Ping, TraceRoute and NS Lookup . . .**

The Ping, TraceRoute and NS Lookup dialog box appears.

Step 2 Select the **NS Lookup** tab.

Step 3 Enter an address or hostname in IPv4Address/Hostname.

Alternatively, click **Select** to choose a host network/host object that defines the IP address.

Step 4 Optionally, to employ a particular DNS server in the lookup, enter the server's name or address in DNS Server.

Step 5 Click **Lookup**.

The system displays the particular address/hostname pair, as well as the DNS server used in the lookup.

Using the Packet Capture Wizard

You can use the Packet Capture Wizard to configure, run, view, and save captures for troubleshooting errors. The captures can be run using preconfigured access lists or using match criteria of packet parameters such as source and destination addresses/ports on one or more interfaces. The wizard runs one capture on each of the ingress and egress interfaces. You can save the captures on the Cisco Security Manager client computer to examine them using a packet analyzer.

The Packet Capture Wizard also supports packet captures on ASA clusters. If you run the Packet Capture Wizard on the control unit of an ASA cluster, you are given the option of capturing data for just the selected device or all devices in the cluster. After running the capture for a cluster, you can view summary information for the cluster and also view or download capture buffers for specific devices in the cluster.



Note

If the control unit has changed, it should be updated in Security Manager before running the Packet Capture Wizard. If not, capture for cluster members will contain errors. You can update the control unit for a cluster using the **Retrieve From Device** button on the **Device Properties > Cluster Information** page. For more information, see [Cluster Information Page, page 3-50](#).

The captures can be run using pre-configured access-lists or using match criteria of packet parameters such as source, destination address/port on one or more interfaces.

Please note the following:

- You can only use the Packet Capture Wizard on firewall devices (PIX, ASA, or FWSM).
- Packet capture based on packet match criteria is only supported on devices running ASA version 7.2(3) or later. For other devices, packet capture can only be performed based on access-lists.

To use the Packet Capture Wizard:

-
- Step 1** Launch the Packet Capture Wizard using one of the following methods:
- Select **Tools > Packet Capture Wizard**.
 - (Device view) Right-click on an ASA, PIX, or FWSM device and select **Packet Capture** on the shortcut menu. Proceed to [Step 3](#).
 - (Event Viewer) Right-click on an event from an ASA, PIX, or FWSM device and select **Packet Capture** on the shortcut menu. Proceed to [Step 3](#).
- Step 2** If you launched the Packet Capture Wizard from the Tools menu, select the device on which you want to capture packets. The Security Devices list contains only devices on which packet capture can be run.
- Step 3** If you selected a device that is the control unit of an ASA cluster, specify whether to run the capture for the selected device only or for the entire cluster, and then click **Next**.
- Step 4** Select the ingress interface from the drop-down list.



Note

You cannot select the same interface as ingress and egress in the same wizard.

- Step 5** In the Packet Match Criteria area, do one of the following:
- To specify the access list to use for matching packets, select the **Access-List** radio button, and then choose the access list from the drop-down list.

- To specify packet parameters, select the **Packet Parameters** radio button and complete the following fields:
 - Specify the source and destination in the Source Host / Network and Destination Host / Network fields, respectively. You can use any of the following to specify the source or destination:
 - Network/host object. Enter the name of the object or click **Select** to select it from a list. You can also create new network/host objects from the selection list.
 - Host IP address, for example, 10.10.10.100.
 - Network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0.
 - Choose the protocol type to capture from the drop-down list. Available protocol types to capture are ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp, or udp.

If the protocol is ICMP, select the ICMP type from the drop-down list. Available types include ALL, alternate-address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute, or unreachable.

If the protocol is TCP or UDP, specify the source and destination port services. Available options include the following:

 - To include all services, choose All Services.
 - To indicate specific services, choose an appropriate operator from the drop-down list (=, !=, >, <, or range) and then select one of the following: aol, bgp, chargen, cifs, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nfs, nntp, pcanewhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, whois, or www. The >, <, and range operators function based on the port number assigned to the selected service.

When using the range operator, a second drop-down list is enabled. Use the two drop-down lists to select the starting and ending services in the range you want to specify. The service with the lower corresponding port number should be selected in the first drop-down list, and the service with higher corresponding port number should be selected in the second drop-down list.

Step 6 Click **Next** to proceed to the Select egress interface step.

Step 7 Select the egress interface from the drop-down list.



Note You cannot select the same interface as ingress and egress in the same wizard.

Step 8 In the Packet Match Criteria area, do one of the following:



Note The Packet Match Criteria option (Access-list or Packet Parameters) you selected for the ingress interface will also be used for the egress interface. Also, if you used packet parameters for matching on the ingress interface, the protocol definition you used will also be used for the egress interface.

- If you are using an access list to match packets, choose the access list from the drop-down list.
- If you are using packet parameters to match packets, the parameters used for ingress are also used for egress.

Step 9 Click **Next** to proceed to the Set buffer parameters step.

Step 10 Specify the buffer parameters by configuring the following fields:

In the Buffer Parameters area, you specify the buffer size and packet size. The buffer size is the maximum amount of memory that the capture can use to store packets. The packet size is the longest packet that the capture can hold. We recommend that you use the longest packet size to capture as much information as possible.

- **Read capture buffer every 10 seconds**—Select this option to automatically retrieve captured data every 10 seconds. You must use the circular buffer when selecting this option.
- **Use a circular buffer**—Select this option to continue capturing packets after the buffer is full. When you choose this setting, if all the buffer storage is used, the capture starts overwriting the oldest packets.
- **Buffer Size**—Enter the number of bytes (between 1534 and 33554432) that the capture can use to store packets.
- **Maximum Packet Size**—Enter the number of bytes (between 14 and 1522) that the capture can use to store a single packet. Use the largest value, 1522, to capture as much information as possible.

Step 11 Click **Next** to proceed to the Summary step, which shows the traffic selectors and buffer parameters that you have entered.

Step 12 Click **Next** to proceed to the Run, View & Save step.

Step 13 From the Run, View & Save step, you can do the following:

- Click **Start Capture** to begin capturing packets.
- Click **Stop Capture** to stop capturing packets.
- To fetch the next set of captured packets, do one of the following:
 - For individual devices, click **Display Capture Packets** to fetch the next set of captured packets from the device and update the buffer status bar. This button is only enabled if the Read capture buffer every 10 seconds option was not selected during the Set buffer parameters step.
 - For clusters, click **Get Cluster Capture Summary** to fetch the next set of captured packets from the devices in the cluster and update the buffer status bar. This button is only enabled if the Read capture buffer every 10 seconds option was not selected during the Set buffer parameters step.
- When running a capture for an ASA cluster, the following options are available for working with the capture buffers of the devices in the cluster:

- To view the captured packets from a device in the cluster, select the device in the Device Name list under Get Capture Buffer, and then click **Get Capture Buffer**.

The capture information for the selected device is displayed. Refer to the other options in this list for the actions you can perform on this data.

- To remove the capture content for a specific device or all devices in the cluster and allow room in the buffer to capture more packets, select the device or **--All--** in the Device Name field under Clear Capture Buffer, and then click **Clear Capture Buffer**.



Note We recommend saving captures prior to clearing the device buffers. If you do not save captures prior to clearing the device buffers, captured data will be lost.

- Click the **Launch Network Sniffer** button above the Ingress Capture window or the Egress Capture window to view the corresponding ingress or egress capture using an external packet analyzer tool. You must have a packet analyzer installed and associated with *.pcap file extension.
- Click **View Data in Larger Window** to view the packet capture data side-by-side in a larger window.
- Click **Save captures** to display the Save Capture dialog box. Choose the format in which you want to include the captures: ASCII or PCAP. You have the option of saving either the ingress capture or the egress capture.
- Click **Clear Device Buffer** to remove the current content and allow room in the buffer to capture more packets.

**Note**

We recommend saving captures prior to clearing the device buffers. If you do not save captures prior to clearing the device buffers, captured data will be lost.

- Click **Refresh Capture Buffers** to fetch the next set of captured packets for a device in a cluster and update the buffer status bar.

Step 14 Click **Finish** to exit the wizard.

IP Intelligence

Network security devices managed by Cisco Security Manager generate large amounts of security logs and security events containing the IP address information of the attacker or victim machines or both.

Useful details about an IP address, collectively referred to as IP intelligence, can be discovered by using tools such as ping, trace route, and NS lookup. Often, however, it is desirable to augment these somewhat rudimentary tools with more advanced tools.

Beginning with Version 4.5, Security Manager provides advanced tools that furnish critical details about an IP address in real time or in generated reports. These critical details are provided by Security Manager in the following categories:

- Reverse DNS (FQDN) Lookup Service
- GeoIP Lookup Service
- Whois Lookup Service

**Note**

IP intelligence for IPv6 addresses is not supported.

These IP intelligence categories are described in the following table:

Table 71-10 IP Intelligence Categories

IP Lookup Provider	Information Source	Real Time or Manual/Limitations
Reverse DNS (FQDN) Lookup Service	DNS servers	Real time Note External DNS configuration is an additional option that you can configure, but you will need to evaluate your individual situation.
GeoIP Lookup Service	External third-party commercial vendor	Real time
Whois Lookup Service	Provided by free whois server, a third-party web server.	Real time Limitations: <ul style="list-style-type: none"> Whois is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. There are five regional internet registry (RIR) organizations that manage the allocation and registration of IP addresses. ARIN (American Registry for Internet Numbers), RIPE (Réseaux IP Européens Network Coordination Centre), and APNIC (Asia-Pacific Network Information Centre) are the 3 RIR's that Security Manager will use to query directly; they also provide the referred URL. For RIPE and APNIC, if there is any parsing error, only the direct URL link will be shown. Clicking on the provided URL will display the details for the given IP address in web browsers. If an IP address belongs to LACNIC (Latin America and Caribbean Network Information Centre) or AfriNIC (African Network Information Centre) , the web browser will display the homepage of the respective RIR. In some cases (such as dns query getting blocked by windows firewall or invalid proxy has configured in the cco settings page) , Whois may not work even though it is enabled. In such scenario as a "Fail-safe" method it will provide only the referred url.

Before you begin looking up IP intelligence, you must enable the necessary services at **Configuration Manager > Tools > Security Manager Administration... > IP Intelligence Settings**. Refer to [IP Intelligence Settings Page, page 11-41](#).

IP intelligence lookup can be done by using any of the following methods:

- Use the IP Intelligence dialog box: Navigate to **Configuration Manager > Tools > IP Intelligence...** and then enter a valid IPv4 address in the search field of the IP Intelligence dialog box that pops up. (You must press **Enter** after typing the IP address.)
- Use "Quick Launch" by mousing over (hovering over) a valid IPv4 address in the Security Manager interface. You can do this in Event Viewer, for example; in general, you can do this in all GUI tables in which an IP address is part of the data displayed. If more than one IP address is displayed in one cell of a GUI table, only the first IP address is displayed.



Note You may experience a second or two of latency with Quick Launch before you see the "IP Intelligence" option in the GUI.



Note You can enable or disable Quick Launch by selecting or clearing the "Enable Quick Launch" check box in the IP Intelligence dialog box at **Configuration Manager > Tools > IP Intelligence....**

- Use the IP Intelligence widget in the Dashboard (**Launch > Dashboard...**). This method is equivalent to using the IP Intelligence dialog box described above.
- Use Report Manager (**Launch > Report Manager...**) to see IP intelligence in any of the following reports:
 - **FW/Summary Botnet**—Top Infected Hosts
 - **FW/Summary Botnet**—Top Malware Sites
 - **FW**—Top Destinations
 - **FW**—Top Sources
 - **IPS**—Target Analysis
 - **IPS**—Top Attackers
 - **IPS**—Top Victims



Note There are several points to note about these reports: 1) They will not contain Whois information. 2) If you have disabled all the providers at **Configuration Manager > Tools > Security Manager Administration... > IP Intelligence Settings**, then none of the IP intelligence-related columns will be displayed in the report. 3) If you enable *all* the services, only the reverse dns (FQDN) and GeoIP details will be displayed in the report. 4) If you enable only *one* service, then that service only will be displayed in the report.



Note The generated report in both PDF and CSV formats will contain the IP intelligence details.



Note All these reports require the necessary services to be enabled. Refer to [IP Intelligence Settings Page, page 11-41](#).

Integrating CS-MARS and Security Manager

While Cisco Security Manager lets you centrally manage security policies and device settings in your network, the Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a separate application that monitors devices and collects event information, including syslog messages and NetFlow traffic records, with much more extensive network monitoring capabilities than Security Manager. CS-MARS aggregates and presents massive amounts of network and security data in an easy-to-use format. Based on information derived from CS-MARS reports, you can edit device policies in Security Manager to counter security threats.

Specifically, if you use Security Manager to configure firewall access rules and IPS signatures, you can configure CS-MARS to collect information related to those policies and make it available to Security Manager users. By registering the CS-MARS servers with Security Manager, users can navigate directly from a specific access rule or IPS signature to a CS-MARS report window, pre-populated with query criteria for that rule or signature.

Similarly, CS-MARS users can view the Security Manager policies related to specific CS-MARS events. This bi-directional mapping of specific events to the policies that triggered them, combined with the ability to immediately modify the policies, can dramatically reduce the time spent configuring and troubleshooting large or complex networks.

To enable this cross-communication, you must register your CS-MARS servers with Security Manager, and register your Security Manager server with the CS-MARS servers. You must also register the specific devices with each application. Then, when working with firewall access rules or IPS signatures for a device, a Security Manager user can quickly view real-time and historical event information related to that rule or signature.

The following sections explain how to enable and use CS-MARS and Security Manager cross-communication:

- [Checklist for Integrating CS-MARS with Security Manager, page 71-36](#)
- [Looking Up CS-MARS Events for a Security Manager Policy, page 71-41](#)
- [Looking Up a Security Manager Policy from a CS-MARS Event, page 71-45](#)

Checklist for Integrating CS-MARS with Security Manager

To enable the cross-communication between CS-MARS and Security Manager (as described in [Integrating CS-MARS and Security Manager, page 71-36](#)), you must identify the applications to each other and ensure that devices managed by both applications are configured appropriately. The following table describes the integration steps.

If you have problems with cross-communications, see [Troubleshooting Tips for CS-MARS Querying, page 71-40](#).

Table 71-11 Integrating CS-MARS and Security Manager

Task	Description
Add the devices to Security Manager and CS-MARS	See Adding Devices to the Device Inventory , page 3-7 for information about adding devices to Security Manager. See the Device Configuration Guide for Cisco Security MARS for information about adding devices to the CS-MARS inventory. A device must be supported by both applications to provide cross-communication for the device. Supported device types generally are those providing Firewall > Access Rules, or IPS > Signatures policies. (These include: PIX, ASA and FWSM appliances, Cisco IOS routers, Cisco IPS sensors and modules, and Cisco Catalyst switches.)
Configure the devices as required by each application	See Chapter 2, “Preparing Devices for Management” for information about basic configuration requirements for Security Manager. See Device Configuration Guide for Cisco Security MARS for the more extensive requirements for CS-MARS.
Register Security Manager with CS-MARS	For information on configuring CS-MARS to communicate with Security Manager, see User Guide for Cisco Security MARS Local and Global Controllers . You might want to create a CS-MARS user account specifically for linking with Security Manager. See Configuring the Security Manager Server to Respond to CS-MARS Policy Queries , page 71-37.
Register CS-MARS controllers with Security Manager	For information on registering CS-MARS controllers with Security Manager, see Registering CS-MARS Servers in Security Manager , page 71-38.
Link CS-MARS controllers to the devices in Security Manager	In Security Manager, you can proactively discover the CS-MARS controllers that monitor a particular device by clicking Discover CS-MARS on the device’s Device Properties page, as described in Discovering or Changing the CS-MARS Controllers for a Device , page 71-39. Otherwise, the appropriate controller is discovered automatically when a user attempts to look up events for the device (the user is prompted to select a controller if more than one monitors the device).

Related Topics

- [Viewing CS-MARS Events for an Access Rule](#), page 71-42
- [Viewing CS-MARS Events for an IPS Signature](#), page 71-44
- [Looking Up a Security Manager Policy from a CS-MARS Event](#), page 71-45

Configuring the Security Manager Server to Respond to CS-MARS Policy Queries

CS-MARS must be allowed access to the Security Manager server so that it can perform policy lookup queries and obtain policy information.

- If you are using Common Services AAA authentication on the server (for example, Cisco Secure ACS), you must update the administrative access settings to ensure that CS-MARS has the necessary client access to the Security Manager server.

- Define a user account in Security Manager that CS-MARS can use to perform queries. A separate account is recommended to provide a specific audit trail on the Security Manager server. This account must be assigned one of the following Common Services roles:
 - Approver
 - Network Operator
 - Network Administrator
 - System Administrator

Users with the Help Desk security level can only view the policy look-up table in CS-MARS; that is, they cannot cross-launch Security Manager to modify policies.

**Note**

When you register a Security Manager server with CS-MARS, if you choose to prompt for Security Manager credentials for policy table look-up, a separate CS-MARS account in Common Services for authentication purposes might not be necessary.

For more information on adding users and associating roles with them in Common Services, see the *User Guide for CiscoWorks Common Services*.

Related Topics

- [Registering CS-MARS Servers in Security Manager, page 71-38](#)
- [Discovering or Changing the CS-MARS Controllers for a Device, page 71-39](#)

Registering CS-MARS Servers in Security Manager

As described in [Checklist for Integrating CS-MARS with Security Manager, page 71-36](#), you must register your CS-MARS controllers with Security Manager to enable cross-communication between the applications if you intend to use the applications together.

Then, when a user looks up events for a device, Security Manager identifies the CS-MARS controller that is collecting events for that device. If more than one CS-MARS controller is collecting events for a device, the user can select which to use. You can also specify the correct CS-MARS controller to use in the Device Properties window for each device. (See [Discovering or Changing the CS-MARS Controllers for a Device, page 71-39](#) for more information.)

**Note**

For information about the CS-MARS versions explicitly supported by Security Manager, see the [Release Notes for Cisco Security Manager](#) for this version of the product. If you do try to use a version that is not explicitly supported, you cannot use CS-MARS versions earlier than 4.3.4 or 5.3.4.

-
- Step 1** Choose **Tools > Security Manager Administration** and select **CS-MARS** in the table of contents to display the [CS-MARS Page, page 11-7](#).
 - Step 2** Click the **Add** button to add a CS-MARS server. The New CS-MARS Device dialog box opens (see [New or Edit CS-MARS Device Dialog Box, page 11-8](#) for detailed information).
 - Step 3** In the New CS-MARS Device dialog box, enter the IP address or fully qualified DNS host name of the server, and a user name and password for logging into the server. If you add a local controller, the user name you enter can be either a local account or a global account. Choose the type of account from the User Type list.

**Tip**

If you are using CS-MARS Global Controllers, add them instead of individual Local Controllers. By adding Global Controllers, Security Manager can identify the correct Local Controller for a device, without you having to add each Local Controller. When you add a Global Controller, do not add the individual Local Controllers monitored by the Global Controller.

Click **Retrieve From Device** to get the server's authentication certificate. Click **Accept** when the certificate is presented to you.

Click **OK** when finished. The New CS-MARS Device dialog box closes and the server is added to the CS-MARS device list.

Step 4 From the **When Launching CS-MARS** list, choose whether you want users to be prompted to log in to the CS-MARS server when they request event status, or whether Security Manager should automatically log in to CS-MARS using the credentials provided when the user logged in to Security Manager.

If you elect to use Security Manager credentials, the necessary user accounts must be configured in CS-MARS. Refer to the CS-MARS documentation for more information.

Step 5 Click **Save** on the CS-MARS page to save your changes.

Discovering or Changing the CS-MARS Controllers for a Device

If you use the Cisco Security Monitoring, Analysis and Response System (CS-MARS) controllers to monitor devices, you can register them in Security Manager and then view syslogs and events that are related to firewall access or IPS signature rules for individual devices.

Security Manager can automatically discover the CS-MARS controllers that monitor a device when you try to view events related to a rule. If more than one controller monitors a device, you are prompted to select which controller to use.

You can also proactively select the CS-MARS controller for a device in its Device Properties window. Similarly, if you ever need to change the CS-MARS controller assigned to a device, you can change the selection in its Device Properties window. This procedure explains how to discover or change the CS-MARS controller for a device from its Device Properties window.

Before You Begin

The CS-MARS controller that monitors the device must already be registered with Security Manager on the CS-MARS administration page (**Tools > Security Manager Administration > CS-MARS**). For more information, see [Registering CS-MARS Servers in Security Manager, page 71-38](#).

Step 1 In Device view, do one of the following in the Device selector to open the Device Properties dialog box:

- Double-click a device.
- Right-click a device and choose **Device Properties**.
- Select a device and choose **Tools > Device Properties**.

Step 2 Click **General** in the table of contents to open the General properties page (see [Device Properties: General Page, page 3-41](#)).

- Step 3** In the CS-MARS Monitoring group, click **Discover CS-MARS**. Security Manager determines which registered controller is monitoring the device, if any. If there are more than one, you are prompted to select which CS-MARS controller to use.
-

Troubleshooting Tips for CS-MARS Querying

Use the following troubleshooting tips to help you identify and resolve problems you might encounter when using CS-MARS and Security Manager together:

- HTTPS is required for communication between the Security Manager server and CS-MARS.
- Interface names are not case-sensitive in Security Manager, but they are in CS-MARS. For example, “outside” and “Outside” are considered exclusive by a CS-MARS appliance, while they are equivalent in Security Manager. Further, syslog messages use lower case for all interface names. As a result, when you perform a query for a Security Manager policy from an event generated in CS-MARS, the interface name logged in the syslog event might not match the interface name in that policy in Security Manager. To avoid this problem, use lower case for all interface names, and in the definition of interface roles, in CS-MARS.
- To query for CS-MARS events from Security Manager policies, the Security Manager client must be on the same side of a network address translation (NAT) boundary as the CS-MARS appliance and the Security Manager server.

Similarly, when the CS-MARS client is not on the same side of a NAT boundary as the CS-MARS appliance and the Security Manager server, you can look up Security Manager policies, but in read-only mode. However, you cannot start the Security Manager client from the read-only policy look-up table. The Security Manager client must be on the same side of the NAT boundary as the CS-MARS appliance and the Security Manager server if you want to start the client from CS-MARS to modify a matching policy.

- For FWSM, PIX and ASA devices on which multiple independent security contexts exist, to query for CS-MARS events, you must define a unique management IP address in Security Manager for each security context. Also, the host name and reporting IP address for each virtual context must be configured before adding it to CS-MARS. Otherwise, event look-up from policies on these contexts fails.
- For all IPS device and service policies, a default signature policy is assigned to the device when you do not discover IPS policies, or when you remove the configured policies from the device. If you try to perform event look-up from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, you can then navigate to events in CS-MARS.
- If object grouping or rule optimization is enabled for an access rule defined in Security Manager and the associated access-list commands on the device do not match the optimized rules, no events are displayed in CS-MARS.
- If logging is not enabled for an access rule, a warning message is displayed, and you can only look up traffic-flow events for those rules.
- When supported by the device, Security Manager uses access-control entry (ACE) hashcodes as additional keywords when querying CS-MARS for syslog messages generated by an ACE, and large access-control lists (ACLs) might contain thousands of such hashcodes. If the number of keywords, or the sum of the number of sources, destinations, and protocols for an ACE or a signature exceeds the query limit of 150, an error message is displayed. The error message indicates the probable cause and recommended action.
- Problems with the synchronization between rules and reported events can occur in the following situations:

- The device has been added to Security Manager, but the configuration or changes to it have not been saved to the database. This is especially true for access rules that have been changed but not deployed since the device was added to CS-MARS.
- Access rules exist on the device for which there are no corresponding rules in Security Manager, and vice versa. Be sure all devices are added to Security Manager, and that access rules are configured on them using Security Manager.
- Traffic in the “wrong” direction triggering events for which there is no defined rule. For example, outbound traffic on a higher-security-level interface on which only inbound-traffic rules have been defined.
- If you perform a policy lookup from CS-MARS and the Security Manager client is active, the query is performed on all policies within the open activity or configuration session plus what is saved in the database (the committed configurations). If the Security Manager client is not active, only committed policies are considered.

Related Topics

- [Checklist for Integrating CS-MARS with Security Manager, page 71-36](#)
- [Looking Up CS-MARS Events for a Security Manager Policy, page 71-41](#)
- [Registering CS-MARS Servers in Security Manager, page 71-38](#)

Looking Up CS-MARS Events for a Security Manager Policy

After you integrate CS-MARS and Security Manager, you can look up events in CS-MARS that relate to specific firewall access rules or IPS signatures.

When CS-MARS receives events, they are parsed, “sessionized,” written to an event buffer, and then written to the database. Sessionizing takes two forms: with a session-oriented protocol, such as TCP, the session encompasses the initial handshake to the connection tear-down; with a sessionless protocol, such as UDP, the session start and end times are based more on first and last packets tracked within a restricted time period—packets that fall outside of the time period are considered parts of other sessions.

Because there is a difference between newly-received and fully processed data, you can look up either real-time or historical events:

- **Real-time**—Because sessionization takes time, keeping an event in cache for up to two minutes, you can use the real-time event query to view events right after parsing, providing access to the most current data received.

When you query for real-time events, the query is run automatically, based on the policy values obtained from Security Manager, and the results are displayed in the CS-MARS Query Results window. This real-time event viewer lets you monitor CS-MARS traffic in near real-time, as raw events streaming to CS-MARS, before they are sessionized, with a maximum delay of five seconds. You also can elect to view the sessionized event stream by clicking Edit in the Query Results window and then choosing “Sessionized events” from the Realtime drop-down menu. Note that more delay is possible when there are many events in a session.

- **Historical**—Historical event reports help you identify trends over longer periods of time than is possible with real-time monitoring. When you query for historical events, the CS-MARS Query Criteria: Result window opens. You can either run the query immediately, or save the criteria as a “report” to run at a later time. For historical events, the Result Format is the All Matching Events option, and the Filter By Time value is set to the previous 10 minutes.

The following topics explain event lookup in more detail:

- [Viewing CS-MARS Events for an Access Rule, page 71-42](#)
- [Viewing CS-MARS Events for an IPS Signature, page 71-44](#)

Viewing CS-MARS Events for an Access Rule

From the **Firewall > Access Rules** policy in Security Manager, you can select an access rule and view related event information in CS-MARS. You can view real-time or historical events matching the rule, the traffic flow, the source address, or the destination address. You can view events for any device that supports access rules, including ASA, PIX, FWSM, routers, and switches.

Firewall access rules are presented in the form of an ordered list or table. When deployed, this policy becomes an access-control list (ACL), with each entry in the list known as an access-control entry (ACE). (For more detailed information, see [Understanding Access Rules, page 16-1](#).)

When deciding whether to forward or drop a packet, a device tests the packet against each access rule in the ordered list. If you enable logging for an access rule, the results of the test are recording according to your per-rule log settings. Some devices, such as ASA, generate log entries for denied access even if you do not configure logging explicitly. For information on creating access rules, including logging options, see [Configuring Access Rules, page 16-7](#).

You can query CS-MARS for real-time or historical events related to an access rule for the following types of traffic. To use the commands, right-click the rule and select them from the context menu.

- **Flow**—A traffic flow is defined by the rule's source and destination IP addresses, protocol, and ports. The reported flow events include connection set-up and tear-down. Logging need not be enabled for the access rule to record this information.

To view flow-related events, use the following right-click commands:

- **Show MARS Events > Realtime > Matching this Flow**—To view real-time query results in CS-MARS for events matching this traffic flow. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
- **Show MARS Events > Historical > Matching this Flow**—Opens the historical query criteria page in CS-MARS with fields populated based on the selected rule's traffic flow. Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query or save it for later submission and re-use.
- **Rule**—If logging is enabled for the rule (in the [Advanced and Edit Options Dialog Boxes, page 16-17](#)), the device sends syslog messages to CS-MARS to record the logged events (assuming CS-MARS monitors the device). This query includes the access-rule parameters, including available keyword information. Reported events do not include connection set-up and tear-down.

To view rule-related events, use the following right-click commands:

- **Show MARS Events > Realtime > Matching this Rule**—To view real-time query results in CS-MARS for events matching this rule (flow parameters plus keywords); results begin scrolling within five seconds. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
- **Show MARS Events > Historical > Matching this Rule**—Opens the historical query criteria page in CS-MARS with fields populated based on the access rule (flow parameters plus keywords). Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.
- **Source or Destination**—If you right-click the Source or Destination cell in an access rule entry, you also can choose to view real-time or historical events matching the rule's source or destination IP address.

To view events for a source or destination address, right-click the address in the Source or Destination cell and choose one of the following commands (the specific command differs depending on the cell you select):

- **Show MARS Events > Realtime > Matching this Source/Destination**—To view real-time query results in CS-MARS for events with a matching source or destination address. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
- **Show MARS Events > Historical > Matching this Source/Destination**—Opens the historical query criteria page in CS-MARS with fields populated based on the access rule's source or destination address. Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.

Security Manager provides the following information to CS-MARS as criteria for a traffic-flow or access-rule event queries:

- Device details—General information about the device, such as host name, domain name, management IP address, and display name.
- Source addresses—Source addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Destination addresses—Destination addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Service—Protocol and port information.
- Event Type—"Built/teardown/permitted IP connection" for permit rules and "Deny packet due to security policy" for deny rules.
- Keyword (rule events only, not provided for traffic-flow queries)—ACL name and ACE hashcode, if available, connected by the logical operator OR.

On Version 7.0 or later PIX and ASA devices, each access rule is assigned an MD5 hashcode, which is included in the syslogs generated by that rule. Large ACLs can include thousands of access rules. Used as query keywords, these hashcodes can help produce more-accurate event matches. If a device does not support hashcodes, a warning is displayed that query results might be inaccurate because of keyword ambiguity; you can proceed with the query, and then edit the query keyword list and resubmit.

Tips:

- You can query on only one access rule at a time.
- When NAT or PAT is configured on a security device, the source and destination addresses are mapped to pre-translation and post-translation addresses, respectively, and the translated addresses are used when Security Manager sends a query to CS-MARS. For inbound access rules, the destination address is considered the pre-translation address, and for outbound access rules, the source address is considered the post-translation address.
- If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.
- Depending on how credentials verification is set up on your system, you might be prompted to log into CS-MARS. For more information, see [Registering CS-MARS Servers in Security Manager](#), page 71-38.

Related Topics

- [Access Rules Page](#), page 16-10

- [Looking Up CS-MARS Events for a Security Manager Policy, page 71-41](#)
- [Viewing CS-MARS Events for an IPS Signature, page 71-44](#)

Viewing CS-MARS Events for an IPS Signature

When an IPS or IOS IPS device detects and reports a network intrusion by comparing incoming traffic to a configured signature, a syslog message is generated on the device. If the device is monitored by CS-MARS, an incident is generated in CS-MARS after the log associated with the signature is obtained from the device. Looking up the events associated with a specific signature lets you quickly identify attacks and tune your device configuration to minimize or prevent intrusions.

To view reported network intrusion events in CS-MARS, you can select one or more entries in the Signatures policy for a device in Security Manager and navigate to the CS-MARS Query page to view real-time and historical events.

When you look up real-time events for a signature, the query is run automatically and the results displayed in CS-MARS. However, when you look up historical events for a signature, the values sent by Security Manager to CS-MARS are used to populate the query fields. You can modify the query fields as desired, and then run the query, or save it for later use.

Security Manager provides the following signature information to CS-MARS as query criteria:

- **Device details**—General information about the device, such as host name, domain name, management IP address, and display name.
- **Keyword**—Signature ID, subsignature ID, and virtual sensor name, if applicable.

For virtual sensors, the name of the sensor is included as a keyword criterion along with other device information and signature parameters.

Related Topics

- [Looking Up CS-MARS Events for a Security Manager Policy, page 71-41](#)
- [Viewing CS-MARS Events for an Access Rule, page 71-42](#)

Step 1 (Device view) With an IPS or IOS IPS device selected, select **IPS > Signatures > Signatures** to display the [Signatures Page, page 39-4](#).

Step 2 Right-click the desired entry in the signatures table, or select multiple entries before right-clicking one of them, and choose one of the following commands from the **Show MARS Events** menu:

- **Realtime**—To view real-time query results in CS-MARS for events matching this signature; results begin scrolling within five seconds. Use this option to view raw events as they stream to CS-MARS. You can change the query criteria in the CS-MARS Query Results window at any time, applying new parameters to alter the real-time results.
- **Historical**—Opens the historical query criteria page in CS-MARS with fields populated based on the signature parameters. Edit the parameters and query criteria as desired, and click Apply to continue. Next, in the Query window, you can submit the query or save it for later submission and re-use. You can edit the query and save it as a report if you want to run it again later.

Tips:

- If a signature is disabled, you are warned and asked if you want to proceed to event lookup.
- If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.

- Depending on how credentials verification is set up on your system, you might be prompted to log into CS-MARS. For more information, see [Registering CS-MARS Servers in Security Manager, page 71-38](#).
 - All custom signatures are categorized as “Unknown Device Event Type” events in CS-MARS.
 - A default signature is assigned to an IPS device if you elect not to discover IPS policies when adding the device to the Security Manager inventory, or when you remove configured IPS policies from the device. If you try to look up events from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, you can then query for related events in CS-MARS.
 - Events of type Packet Data and Context Data are not displayed in the query results because these events are not triggered by signature rules.
-

Looking Up a Security Manager Policy from a CS-MARS Event

The *User Guide for Cisco Security MARS Local and Global Controllers* contains detailed information about how to look up policies based on events shown in CS-MARS. The information includes extensive troubleshooting information to help resolve any problems you might have, plus a checklist of what you must configure in CS-MARS to enable the interaction.

The main reason you would want to perform policy lookup is to adjust a policy based on the events that it is generating. For example, an access rule might be dropping traffic that you actually want to allow. Because you are looking at the event, you know there is a policy that is causing the event, so with a few clicks, you can get from that event to the policy you need to reconfigure.

The general process for looking up a policy based on a device-generated event is as follows. Note that the Security Manager client must be installed on your system to perform policy lookup.

Related Topics

- [Viewing CS-MARS Events for an Access Rule, page 71-42](#)
 - [Viewing CS-MARS Events for an IPS Signature, page 71-44](#)
-

Step 1 Find the event in CS-MARS in the Query Results or Incident Details pages.

For more information on the syslog and NetFlow events you can use for querying access rules, see the following topics:

- [System Log Messages Supported for Policy Look-up, page 71-46](#)
- [NetFlow Event Reporting in CS-MARS, page 71-47](#)

Step 2 Click the Security Manager icon in the Reporting Device cell for the event. You might be prompted to log into Security Manager, based on how you configured CS-MARS.

If more than one device in Security Manager matches the event characteristics, you are prompted to select a device.

Step 3 Detailed information is obtained from Security Manager and presented based on whether the event is for an access rule or IPS signature:

- **Access rule**—The access rules are displayed in CS-MARS in a read-only window with the rule that matches the event highlighted.

If you decide to edit a rule, click the rule number, and you are taken to the rule in the Access Rule policy in the Security Manager client. You can then make your edits, save them, and then deploy configurations. Remember that your changes are not made to the device until you deploy them.

For more information on configuring access rules, see [Configuring Access Rules, page 16-7](#).

- **IPS Signature**—Signature details are displayed in CS-MARS in a read-only window.

To edit the signature, click **Edit Signature**, and you are taken to the signature in the Signatures policy, where you can make your changes. For more information, see [Editing Signature Parameters \(Tuning Signatures\), page 39-23](#).

If you decide you want to instead remove specific actions from an event, or remove the event entirely, and prevent further processing by the sensor, click **Add Filter**. This opens the Add Event Filter dialog box in Security Manager, where you can configure an event filter. For more information, see [Filter Item Dialog Box, page 40-9](#).

As with access rules, your changes do not take effect until you deploy the new configuration.

System Log Messages Supported for Policy Look-up

When you configure access rules on security appliances and IOS devices, you can configure logging options in the [Advanced and Edit Options Dialog Boxes, page 16-17](#) that generate system log (syslog) messages. On devices with multiple contexts, each security context includes its own logging configuration and generates its own messages. If Security Manager is configured to interoperate with CS-MARS, these messages are reported to CS-MARS and you can query for the reported information on a per-rule basis.

For additional information about each of these message IDs, see the System Message Guide of the relevant product documentation.

Security-appliance messages

Security-appliance syslog messages begin with a percent sign (%) and are structured as follows:

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

For example:

```
%ASA-2-302013: Built outbound TCP connection 42210
for outside:9.1.154.12/23 (9.1.154.12/23) to inside:2.168.154.12/4402
(192.168.154.12/4402)
```

Note that additional information, such as date and timestamp, precedes these messages. The specific additional information depends on the type of device.

A unique six-digit number identifies each message (*302013* in the preceding example). The following security-appliance syslog message IDs are supported for Security Manager-to-CS-MARS queries. If you change the logging level of a security appliance, be sure these messages are generated at the new level.

Message ID	Message
106023	An IP packet was denied by the access rule. This message is recorded even if logging is not enabled for the rule; this is the Default Logging option.
106100	An IP packet was permitted or denied by the access rule. Additional information is provided, based on the logging level defined for the rule in the Advanced and Edit Options Dialog Boxes, page 16-17 .
302013	A TCP connection between two hosts was created.

302014	A TCP connection between two hosts was torn down.
302015	A UDP connection between two hosts was created.
302016	A UDP connection between two hosts was torn down.
302020	A ICMP connection between two hosts was created.
302021	A ICMP connection between two hosts was torn down.

Router messages

On Cisco IOS routers, syslog messages are also generated for access rules. The first packet that triggers the access list causes an immediate logging message, and subsequent packets are collected over five-minute intervals before they are displayed or logged. Each logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior five-minute interval.

The following IOS syslog message IDs are supported for Security Manager-to-CS-MARS queries.

%SEC-6-IPACCESSLOGP	A packet matching the log criteria for the given access list was detected: TCP and UDP.
%SEC-6-IPACCESSLOGS	A packet matching the log criteria for the given access list was detected: IP address.
%SEC-6-IPACCESSLOGDP	A packet matching the log criteria for the given access list was detected: ICMP.
%SEC-6-IPACCESSLOGNP	A packet matching the log criteria for the given access list was detected: all other IPv4 protocols.



Note

If an excessive number of syslog messages are being generated and reported to CS-MARS, use the [Advanced and Edit Options Dialog Boxes, page 16-17](#) to change the logging level for those access rules that are producing the largest number of messages. You can also look at changing the logging policies on the device to limit the types of messages generated.

NetFlow Event Reporting in CS-MARS

Event reporting in CS-MARS can include NetFlow events from an ASA 8.1+ device.

NetFlow Security Event Logging uses NetFlow version 9 fields and templates to efficiently deliver security telemetry in high-performance environments. NetFlow Security Event Logging scales better than syslog messaging, while offering the same level of detail and granularity in logged events. The ASA NetFlow implementation exports only significant events in the life of a flow, rather than exporting data about flows at regular intervals. The following flow events are exported:

- Flow creation
- Flow tear-down
- Flows denied by an access rule

The ASA also exports syslog messages that contain the same information. If you enable NetFlow on a device, you can consider disabling the equivalent syslog messages. Disabling equivalent syslog messages can help avoid the potential performance degradation caused by generating and processing both NetFlow records and syslog messages representing the same event. The following table lists syslog

messages with an equivalent NetFlow event; the NetFlow Event IDs and Extended Event IDs are included. For information on how to disable NetFlow equivalent syslog messages, see [Server Setup Page, page 53-21](#).

Syslog ID	Syslog Description	NetFlow Event ID	Extended Event ID
302013 302015 302017 302020	TCP, UDP, GRE, and ICMP connection creation.	1 = Flow Created.	0 = Ignore.
302014 302016 302018 302021	TCP, UDP, GRE, and ICMP connection tear-down.	2 = Flow Deleted.	0 = Ignore, or > 2000 = ASP drop reasons.
710003	An attempt to connect to the device's interface was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
106015	A TCP flow was denied because the first packet was not a SYN packet.	3 = Flow Denied.	1004 = Flow denied because first packet was not a TCP SYN packet.
313001	An ICMP packet to the device was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
313008	An ICMP v6 packet to the device was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
106023	A flow was denied by an access list attached to an interface with the access group command.	3 = Flow Denied.	1001 – Flow denied by Ingress ACL. 1002 – Flow denied by Egress ACL.
106100	An access rule was hit.	1 = Flow Created (if ACL permitted the flow). 3 = Flow Denied (if ACL denied the flow).	0 – If Flow permitted by ACL. 1001 – Flow denied by Ingress ACL. 1002 – Flow denied by Egress ACL.

For the Flow Denied NetFlow event, an Extended Event ID indicates the reason for denial, as shown in the following table.

Extended Event ID	Event	Description
1001	FLOW DENIED	The flow was denied by an Ingress ACL.
1002	FLOW DENIED	The flow was denied by an Egress ACL.

Extended Event ID	Event	Description
1003	FLOW DENIED	The security appliance denied an attempt to connect to the interface service. For example, this message appears (with the service SNMP) when the security appliance receives an SNMP request from an unauthorized SNMP management station.
1004	FLOW DENIED	The flow was denied because the first packet was not a TCP SYN packet.
> 2000	FLOW DELETED	Values above 2000 represent various reasons for a flow being terminated.

