



# CHAPTER 21

## Using Monitoring, Troubleshooting, and Diagnostic Tools

---

High network availability is a requirement for large enterprises and service providers. Network managers face various challenges to providing high 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 following topics describe using the monitoring, troubleshooting and diagnostic tools available in Security Manager:

- [Device Managers, page 21-1](#)
- [Performance Monitor as a Status Provider, page 21-7](#)
- [IPS Event Viewer, page 21-12](#)
- [Integration of CS-MARS and Security Manager, page 21-16](#)

## Device Managers

Security Manager can launch device managers for all supported devices, including PIX firewalls, Firewall Services Modules (FWSMs), IPS devices, IOS routers, and Adaptive Security Appliance (ASA) 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.



### Note

---

You cannot launch device managers for any virtual sensors you may have defined on your IPS devices.

---

Security Manager includes device-manager images for the supported devices. This means the device manager need not be installed on the particular device in order to be launched from Security Manager. Access to the correct device manager, and subsequent communications with the selected device, are completely transparent. Further, 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.

Each version of a device manager is compatible with specific versions of software running on the relevant device. Security Manager launches the most-recent available version supported by the software on the device. If a device manager is not available for a particular device software version, an error message is displayed.

Security Manager starts only one instance of device manager per device, and closes the device manager when you exit Security Manager, or the idle-session timeout period is exceeded.

**Note**

You can use a device manager started from Security Manager to view the existing device configuration and to monitor current status, but you cannot use it to apply configuration changes to the device.

Also, although you can modify device configurations directly using an external device manager running on the device, if the device will be managed by Security Manager, we recommend that you do not make changes to a device configuration outside of Security Manager; that is, do not make “out-of-band” changes.

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

**Table 21-1** Device Managers Available in Security Manager

Device Manager	Description
IDM	<p>The IPS Device Manager (IDM) lets you monitor IPS sensors and modules that are part of the Security Manager inventory.</p> <p><b>Note</b> If you access the online help for IDM 5.1, you may be asked to provide user-access information. Enter your user name and password and click OK. This behavior differs from later versions where you are not prompted for credentials.</p> <p>See the <a href="#">IDM documentation</a> for more information about using this device manager.</p>
PDM	<p>The PIX Device Manager (PDM) lets you monitor early FWSMs and PIX 6.x devices; specifically FWSM releases 1.1, 2.2 and 2.3 in single- or multiple-context modes, and PIX OS versions 6.0 through 6.3.</p> <p>See the <a href="#">PDM documentation</a> for more information about using this device manager.</p>
ASDM	<p>The Adaptive Security Device Manager (ASDM) lets you monitor ASA 5500 series, PIX 7.x+, and FWSM 3.x+ devices.</p> <p>See the <a href="#">ASDM documentation</a> for more information about using this device manager.</p>
SDM	<p>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.</p> <p>See the <a href="#">SDM documentation</a> for more information about using this device manager.</p>

**Related Topics**

- [Working with Devices and Device Managers, page 21-3](#)
- [Starting A Device Manager, page 21-4](#)
- [Navigating to an Access Rule from ASDM, page 21-5](#)
- [Navigating to an Access Rule from SDM, page 21-6](#)

## Working with Devices and Device Managers

This section contains information about preparing devices for access by device managers launched from Security Manager. Information about system limits on the number of concurrent connections is also provided.

**Note**

---

All users associated with any of the CiscoWorks Common Services roles (except the Help Desk role, or any of the predefined Cisco Secure ACS roles) have permission to start device managers from Security Manager.

---

Before launching a device manager from Security Manager, please ensure the following preparations have been made:

- Verify SSL/HTTPS is 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 5-1](#) for more information.
- DES encryption is not supported by CiscoWorks Common Services version 3.0 and later. Please ensure that all PIX and ASA devices you intend to manage with Security Manager have a 3DES/AES license. Refer to the device documentation for specific instructions on obtaining a new license.
- You may need to modify Cisco Security Agent, or other anti-virus and network firewall software, on the Security Manager system to allow the device manager service (`xdm-launcher.exe`) to be launched.
- Ensure that Security Manager is correctly configured for contacting and communicating with target devices. Specifically verify device properties such as identity, operating system and credentials. Select the desired device and choose Device Properties from Security Manager's Tools menu (or simply double-click the device) to open the Device Properties window. Verify the settings on the General and Credentials pages. See [Testing Device Connectivity, page 6-15](#) for more information.
- 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.

Please consider the following when launching multiple device managers:

- Starting multiple device managers may 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.

**Note**

With most device managers, you can access the Command Line Interface (CLI) on the device to run various `show` commands to view pertinent information about the device configuration. (This is usually available from the Tools menu of the device manager.) Remember, only `show` commands can be run; you cannot execute other commands on the device from the device manager.

**Related Topics**

- [Device Managers, page 21-1](#)
- [Starting A Device Manager, page 21-4](#)
- [Navigating to an Access Rule from ASDM, page 21-5](#)

## Starting A Device Manager

You can start device managers for all devices (both static and dynamic IP addresses) that are supported by Security Manager. You can run multiple device managers at the same time, but only one device manager per device. (However, multiple Security Manager clients can each be running a device manager for the same device.) Each device manager opens in a separate window, and you can switch between Security Manager and the device manager windows at any time. When you exit Security Manager, all device manager windows are closed.

**Note**

Generally, the credentials supplied when the device was added to the Security Manager inventory are used to start the device manager. (Some versions of SDM require that you enter a user name and password when the device manager is started.)

If valid device credentials are not available when starting a device manager, an error message is displayed. Choose Device Properties from the Tools menu, (or simply double-click the device in the Device selector) to open the Device Properties page, then select Credentials to add credential information for the selected device.

**Related Topics**

- [Device Managers, page 21-1](#)
- [Working with Devices and Device Managers, page 21-3](#)

Follow these steps to launch a device manager:

**Procedure**

**Step 1** In Device View, select a device and then do one of the following:

- Choose **Device Manager** from the Tools menu.
- Right-click the device and select **Device Manager** from the pop-up menu.

You are warned that a Security Manager-launched device manager cannot make any configuration changes. You can select **Do not show this again** in the dialog box to turn off this warning for subsequent device-manager launches.

- Step 2** When you launch a device manager from Security Manager, the device manager service, `xdm-launcher.exe`, is started. You may have to expressly allow this action, if your installed anti-virus and intrusion-prevention software (e.g., Cisco Security Agent) attempts to prevent execution of `xdm-launcher.exe`.
- A progress bar is displayed; the device manager windows opens when the start operation is complete.
- 

## 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, page K-131](#)), and the individual access rules must be configured to generate log messages when they are matched (in the [Advanced Dialog Box, page I-8](#)).

---

You can monitor syslog messages in device managers launched from Security Manager, and for certain device managers, you can 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 via SDM for all managed routers running IOS, and via ASDM for managed PIX and ASA version 8.0(3) devices, and FWSM version 3.1 and 3.2 blades.

### Related Topics

- [Navigating to an Access Rule from ASDM, page 21-5](#)
- [Navigating to an Access Rule from SDM, page 21-6](#)

## 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 Dialog Box, page I-8](#)), 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 21-5](#)
- [Navigating to an Access Rule from SDM, page 21-6](#)

#### Procedure

- 
- Step 1** Select a PIX, ASA, or FWSM in the Security Manager device inventory.
- Step 2** Choose **Device Manager** from the Tools menu to launch ASDM. For more information about starting device managers, see [Starting A Device Manager, page 21-4](#).
- 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 21-5](#)
- [Navigating to an Access Rule from ASDM, page 21-5](#)

#### Procedure

- 
- Step 1** Select an IOS router in the Security Manager device inventory.
- Step 2** Choose **Device Manager** from the Tools menu to launch SDM. For more information about starting device managers, see [Starting A Device Manager, page 21-4](#).
- 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.

---

## Performance Monitor as a Status Provider

In addition to the device summaries displayed in the [Inventory Status Window, page C-37](#), Security Manager lets you add and configure “status providers” that collect information about various events from external sources. Specifically, you can configure Security Manager to collect and display information from up to five Cisco Performance Monitor servers. Additionally, you can configure the same status provider to send event details to multiple Security Manager servers.

Your Security Manager license grants you the right to download, install and use Performance Monitor. Cisco Performance Monitor is a tool that monitors device performance and VPN statistics. Supported services are remote-access VPN, site-to-site VPN, firewall, Web server load-balancing, and proxied SSL.

For Performance Monitor information to be collected and reported in Security Manager, you must perform the following general steps:

- **Add each device to the Security Manager inventory**

See [Adding Devices to the Device Inventory, page 6-7](#) for specific instructions. Note that you can check Security Manager's connection with the currently selected device at any time by clicking the `Test Connectivity` button on the Credentials page of the Device Properties window. (Choose Device Properties from Security Manager's Tools menu; select Credentials in the Device Properties window.)

- **Configure each device for monitoring**

Devices in the Security Manager inventory must be configured to allow access by Performance Monitor, and to provide essential information by means of SNMP traps, syslog messages and device polling. Refer to [Preparing Devices for Monitoring, page 21-8](#) for more information.

- **Add each device to the Performance Monitor inventory**

Refer to [About Adding Devices to Performance Monitor, page 21-9](#) for additional information.

- **Register Performance Monitor as a status provider in Security Manager**

This procedure establishes communications between Security Manager and the Performance Monitor server, and is described in [Configuring Status Providers, page 21-10](#). You can register up to five Performance Monitor servers in Security Manager.

Security Manager establishes an SSL connection with each registered Performance Monitor, and after authenticating the Performance Monitor credentials, Security Manager begins to receive status reports.

If a device is deleted from Performance Monitor but is still available in Security Manager, or if you exclude the device from Performance Monitor polling, the device health and performance reports are no longer available in Security Manager.

#### Related Topics

- [Viewing Inventory Status, page 6-25](#)
- [Viewing Monitored Events, page 21-11](#)

## Preparing Devices for Monitoring

To enable status reporting, devices in the Security Manager inventory must be configured to allow access by Performance Monitor, and to provide essential information by means of SNMP traps, syslog messages, and device polling.

The following sections outline the steps to take for various devices:

- **SSL Services Modules**
- **IPSec VPN Shared Port Adapters (VPN SPAs)**
- **Catalyst 6500 Switches**
- **Routers**
- **FWSM, ASA and PIX devices**

Refer to the “Bootstrapping Devices” section of the [User Guide for Cisco Performance Monitor](#) for additional information about these steps.

#### SSL Services Modules

Generate an RSA key and enable SSH on the services module.

Confirm that an administrative user account exists on the SSL module, and configure an enable password.

#### IPSec VPN Shared Port Adapters (VPN SPAs)

Enable HTTPS.

#### Catalyst 6500 Switches

Enable SNMP and set up community strings. SNMP is required for polling and monitoring.

**Caution**

---

SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic.

---

Enable SNMP traps for CSM services modules. Enter the actual numeric IP address of the server on which you installed Performance Monitor.

**Routers**

Enable SNMP and set up community strings. SNMP is required for validation, polling, and monitoring.

**Caution**

---

SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic.

---

Enable SNMP traps. Enable HTTPS.

**FWSM, ASA and PIX devices**

Specify the Performance Monitor server as an SNMP host for firewall appliances, devices, and modules.

**Caution**

---

SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic.

---

Specify the Performance Monitor server as the HTTP host for polling. Enable HTTPS polling. Configure syslog traps.

**Note**

---

Performance Monitor stops polling all devices that are enabled for monitoring when one device takes more than 30 seconds to return results. When Performance Monitor tries to retrieve the output of show commands from devices using HTTPS, retrieval of a single show command on a device might take more than 30 seconds, causing stoppage of polling. This problem might occur if Performance Monitor polls the device over a very slow WAN link. You can change the polling timeout value in Performance Monitor.

---

**Related Topics**

- [Viewing Monitored Events, page 21-11](#)
- [User Guide for Cisco Performance Monitor](#)

## About Adding Devices to Performance Monitor

A device must be added to the inventories of both Security Manager and Performance Monitor before its status can be displayed in Security Manager's Inventory Status window. Adding a device to the Security Manager inventory is described in [Adding Devices to the Device Inventory, page 6-7](#).

In Performance Monitor, a device is either a physical node in the network, or it is a virtual node that is defined by a physical node. In either case, the device must have a static IP address. You can import the following devices into Performance Monitor:

- FWSM, PIX, and ASA appliances
- SSL service modules
- Catalyst 6500 with CSM or VPN modules
- VPN routers

**Note**

For multiple-context devices, you import only the admin context; Performance Monitor will monitor every configured context on the physical device.

There are three methods for adding devices to Performance Monitor:

- Import device attributes from a comma-separated value (CSV) file. Enter or Browse for the file name, and then select the device or devices to be imported.
- Enter device attributes manually. Choose the device type, enter the fully qualified device name or IP address, and then enter the SNMP attributes and device-access credentials (or in the case of an SSL module, the SSH credentials).
- Import device attributes from a Device Credentials Repository (DCR) on a Common Services-based server. Provide DCR repository host access information (fully qualified server name or IP address, and user name and password for access), and then select the device or devices to be imported.

**Note**

The device to be imported must be a type supported by both Security Manager and Performance Monitor. You cannot import any device when the MCP process has stopped. You also cannot import any device that uses a dynamic IP address, or that lacks configured SNMP values.

During the device-import process, Performance Monitor confirms that the device exists and is reachable, that it has the required features and interfaces enabled, has the correct credentials, uses a static (non-dynamic) IP address, and has SNMP configured. Following this device validation, Performance Monitor sets the device to a managed state by default, meaning that polling is enabled. For more information on how to add and manage devices in Performance Monitor, see the [User Guide for Cisco Performance Monitor](#).

**Note**

You also can create device groups to interact with multiple devices in a single operation. A device group in Performance Monitor is a named entity that can contain devices, other groups, or a combination of devices and groups.

**Related Topics**

- [Viewing Monitored Events, page 21-11](#)
- [User Guide for Cisco Performance Monitor](#)

## Configuring Status Providers

Effective network management requires rapid identification and resolution of events on mission-critical systems. To aid network monitoring and troubleshooting, Security Manager collects configuration information about the devices in its inventory, and provides summaries of these devices in the Inventory Status window (see [Viewing Inventory Status, page 6-25](#)).

You also can view status information obtained from Cisco Performance Monitor, if your system is configured appropriately. (Performance Monitor is part of the Cisco Security Management Suite.) As a registered status provider, Performance Monitor collects event information for VPN, firewall, load-balancing, and SSL services, and reports it to Security Manager.

To enable Security Manager to collect status information from your Performance Monitor servers, you must register them with Security Manager. You can add up to five such servers to Security Manager. This procedure explains how to register a Performance Monitor server as a status provider.

**Related Topics**

- [Viewing Inventory Status, page 6-25](#)
- [Inventory Status Window, page C-37](#)

**Procedure**

- 
- Step 1** Choose **Security Manager Administration** from the Tools menu to open the Cisco Security Manager Administration window.
- Step 2** Select **Status** from the table of contents in the Administration window to view the [Status Page, page A-37](#).
- Step 3** To add a Performance Monitor server, click the **Add** button; the Add Status Provider dialog box opens.
- Step 4** The key fields in this dialog box are:
- Provider name, short name – These are the names displayed in Security Manager. They do not need to match anything configured on the device.
  - Server – The IP address or fully qualified host name of the Performance Monitor server.
  - User name, password, confirm password – A user account that can log into the Performance Monitor server.
- You can change the other fields as needed for your installation. For a detailed explanation of the fields, see [Add or Edit Status Provider Dialog Box, page A-38](#).
- Click **OK** when finished; the Performance Monitor is added to the Providers list.
- Step 5** Click **Save** on the Status page to save your changes.

**Tip**

You can selectively disable or enable Performance Monitor servers on this page by changing the setting in the Status column. This allows you to temporarily discontinue polling a server for status without deleting its registration.

---

## Viewing Monitored Events

After Performance Monitor and Security Manager are configured for event reporting, Performance Monitor collects information such as VPN tunnel up/down status, device reachability, and CPU usage threshold, and reports it to Security Manager.

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. However, you can configure thresholds in Performance Monitor, and only events exceeding specified thresholds are displayed.

You can view reported events in Security Manager, as follows:

1. Choose **Inventory Status** from the Tools menu to open the Inventory Status window.
2. Click the **Status** tab in the lower pane to view Performance Monitor reports.
3. Select the device of interest in the upper pane of the Inventory Status window.

Events for that device are organized by event type. Click the arrow by a type to expand or collapse that list. Similarly, you can expand and collapse the details list by clicking the arrow next to an event name. Event details include timestamp, description, and recommended action.

**Note**

Security Manager displays only the most-recent event of each type. That is, Security Manager does not accumulate the events reported by status providers at different points in time.

For example, assume that at 12:00 noon, Performance Monitor logs a “Device” event with “Critical” severity and an “Interface” event at “Warning” severity, and no events of either type have occurred since then. In this case, both events are displayed. However, if Performance Monitor then logs a “Device” event at “Warning” severity at 1:00 p.m. and another “Critical” Device event at 2:00 p.m., the “Critical” event at 2:00 p.m. is the only Device event retained and displayed.

Refer to the Performance Monitor service for a running history of device events.

The mapping between event severity levels in Performance Monitor and the corresponding event status levels displayed in the Inventory Status window is as follows:

- P1, P2 – Critical events
- P3 – Major events
- P4 – Minor events
- P5 – Warning events

**Related Topics**

- [Viewing Inventory Status, page 6-25](#)
- [Inventory Status Window, page C-37](#)

## IPS Event Viewer

The Cisco IPS Event Viewer (IEV) provides monitoring for small-scale Intrusion Prevention System (IPS) deployments, providing the following capabilities:

- Support for IPS v6 through SDEE compatibility
- Customized reporting
- Configurable notifications such as email and paging
- Visibility into applied-response actions, virtual sensor ID, learned DST OS, and threat rating

The IPS Event Viewer is a Java-based application that lets you view and manage alerts for up to five sensors, reporting the top alerts, attackers, and victims over a specified number of hours or days. You can connect to and view alerts in real time, or via imported log files; you can configure filters and views to help you manage the alerts; and you can import and export event data for further analysis. IEV also provides access to MySDN for signature descriptions.

**Note**

The Cisco IPS Event Viewer and MySQL services must be running on an IEV server (usually the Security Manager server) to enable IEV to monitor sensors. The IEV server retrieves the events from IPS sensors and stores them in the MySQL database. When you start the IEV client from Security Manager, IEV reads the event details from the MySQL database, and displays event data in various views, tables and graphs.

The IPS Event Viewer is installed with Security Manager, and you can start IEV from Security Manager as a client application. Security Manager will start only one instance of IEV; the IEV window closes when you exit the Security Manager client, or when the idle session time-out period is exceeded.

See the Cisco IPS Event Viewer documentation for more information.

#### Related Topics

- [Chapter 13, “Managing IPS Services”](#)
- [Using the IPS Event Viewer with Security Manager, page 21-13](#)
- [Starting the IPS Event Viewer, page 21-13](#)

## Using the IPS Event Viewer with Security Manager

Please be aware of the following when using IEV with Security Manager:

- You can start only one instance of IEV from each Security Manager client.
- If your Security Manager client is running on the same host as the Security Manager server, you cannot use IEV.
- You cannot start IEV from Security Manager on a system on which the Symantec Client Firewall Port Scanning Module or the Symantec Secure Port application is running.
- If you installed the IEV server as part of the Security Manager installation, you cannot install IEV from another source (such as `cisco.com`) on the same system.
- Similarly, if you installed the IEV server as part of the Security Manager installation, it is not re-installed when you re-install Security Manager.
- All IEV client-side run-time files, such as client log files and cache files, are copied to the `\cache\` subdirectory under your local Security Manager client directory. The default location for these files is `C:\Program Files\Cisco Systems\Cisco Security Manager Client\cache\`.
- Backing up and restoring the Security Manager database does not affect the IEV database.

#### Related Topics

- [IPS Event Viewer, page 21-12](#)
- [Starting the IPS Event Viewer, page 21-13](#)

## Starting the IPS Event Viewer

This procedure describes how to launch the IPS Event Viewer (IEV) from Security Manager.



Ethereal is a network protocol analyzer for Windows that lets you examine data from a live network, or from a captured file. You can interactively browse the captured data, viewing summary and detail information for each packet, including the reconstructed stream of a TCP session. If you have Ethereal installed on the same host as IEV, you can start the Ethereal application from the IEV Tools menu and view IP log files. Also, if you have configured the sensor `capturePacket` parameter, IEV uses Ethereal to display the trigger packet.

If Ethereal is installed on your system, to use it with IEV, you must specify the directory where Ethereal

is installed (choose **Edit > Application Settings** in IEV). You also must specify its location if you install Ethereal after installing Security Manager, or if you later move the Ethereal executable file to a different directory.

---

**Related Topics**

- [IPS Event Viewer, page 21-12](#)
- [Using the IPS Event Viewer with Security Manager, page 21-13](#)
- [Accessing Signatures from IPS Event Viewer, page 21-14](#)

**Procedure**

- 
- Step 1** Choose **IPS Event Viewer** from the Security Manager Tools menu.
- The IEV window opens. If it does not, verify the Windows Service, *Cisco IPS Event Viewer*, has started on the Security Manager server.
- Step 2** You can add up to five IPS sensors to view in IEV. From the IEV File menu, choose **New > Device** (or simply press Ctrl-D) to open the Device Properties dialog box.
- Before IEV can receive events from a sensor, you must use the Device Properties dialog box to add the sensor to the list of devices that IEV monitors, and to specify the device-access credentials. You must also add the sensor to the Security Manager inventory to view event data from the sensors you are monitoring.
- Refer to the IEV online Help for additional information about the IEV Device Properties dialog box.
- Step 3** To stop receiving reports from a sensor, you must remove the sensor from the list of devices that IEV monitors. Right-click the device in the Devices tree in the upper-left pane of the IEV window and choose **Delete Device**.
- 

## Accessing Signatures from IPS Event Viewer

Sensors use signatures to determine whether the contents of network packets meet the criteria of an attack. A signature represents a pattern of traffic, often thought of as a set of rules, that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. The Signatures policy page in Security Manager lets you configure signatures for your IPS sensors. Then when processed packets match a given signature rule, the sensor generates an alarm.

You can configure the IPS Event Viewer (IEV) to view and organize alarms from up to five devices. IEV then receives event reports from each sensor, where an event is an IPS message that contains an alert, a block request, a status message, or an error message.

Within IEV launched from Security Manager, you can select an IPS signature from the log of events displayed in IEV's Realtime Dashboard or View folders, and then navigate to the signature policy in Security Manager for that specific event. You can then edit the signature properties to modify the action the sensor must take. The following sections describe navigating to the Signatures page in Security Manager from IEV:

- [Accessing Signatures from the IEV Realtime Dashboard, page 21-15](#)
- [Accessing Signatures from the IEV Views Display, page 21-15](#)

## Accessing Signatures from the IEV Realtime Dashboard

You can use the IEV Realtime Dashboard to view a continuous stream of real-time events from a sensor. By default, the Realtime Dashboard displays the most recent events received from every device configured in IEV. You can configure the Realtime Dashboard to display only events from a particular device, or only events of a particular severity level. You can also configure how often the Realtime Dashboard retrieves events from each sensor, and the maximum number of events displayed.

Refer to the IEV online Help for additional information about using the IEV Realtime Dashboard.

This procedure describes how to access an IPS signature on Security Manager's Signatures page from IEV's Realtime Dashboard:

### Related Topics

- [Accessing Signatures from the IEV Views Display, page 21-15](#)
- [Accessing Signatures from IPS Event Viewer, page 21-14](#)

### Procedure

- 
- Step 1** If you have not done so already, launch IEV from Security Manager. See [Starting the IPS Event Viewer, page 21-13](#) for instructions.
- Step 2** Choose **Tools > Realtime Dashboard > Launch Dashboard**.
- The Realtime Dashboard appears and displays the events received by the sensor since the dashboard was opened.
- Step 3** To view the Security Manager signature policy associated with an event, right-click the row associated with the event and choose **Go to CSM**. The Security Manager window is activated and the Signatures page is displayed, with the IPS signature that generated the event highlighted in the policy table.



---

**Note** For an event entry in IEV, Security Manager searches all the signatures within the context of your current login session (in non-Workflow mode), or your current activity, including policies defined in your private view and saved locally on the client (in Workflow mode). If the event was triggered by a signature not referenced in the current activity, an error message is displayed.

---

You can then edit the signature that triggered the event by clicking the **Edit Row** button.

---

## Accessing Signatures from the IEV Views Display

The IEV's Views tab lets you access various tables and graphs that provide specialized views into event data from a specific source. The IEV ships with five default views; however, you can use the View Wizard to create and store additional views in the Views folder.

You can navigate to events from the data entries in any view. For example, you might select the view that groups events by signature name. You can expand an event to view its details, such as signature name and severity level, and you can then navigate to the related Signatures policy in Security Manager.

Refer to the IEV online Help for additional information about using the IEV Views display.

This procedure describes how to access an IPS signature on Security Manager's Signatures page from IEV's Views display:

**Related Topics**

- [Accessing Signatures from the IEV Realtime Dashboard, page 21-15](#)
- [Accessing Signatures from IPS Event Viewer, page 21-14](#)

**Procedure**

- 
- Step 1** If you have not done so already, launch IEV from Security Manager. See [Starting the IPS Event Viewer, page 21-13](#) for instructions.
- Step 2** If Views is not the active display, click the **Views** tab to display the list of available views.
- Step 3** To open a specific view, double-click its name in the View list.  
The alert aggregation table for that view appears in the view pane on the right.
- Step 4** To view the Security Manager signature policy associated with an event, right-click the row associated with the event and choose **Go to CSM**. The Security Manager window is activated and the Signatures page is displayed, with the IPS signature that generated the event highlighted in the policy table.




---

**Note** For an event entry in IEV, Security Manager searches all the signatures within the context of your current login session (in non-Workflow mode), or your current activity, including policies defined in your private view and saved locally on the client (in Workflow mode). If the event was triggered by a signature not referenced in the current activity, an error message is displayed.

---

You can then edit the signature that triggered the event by clicking the **Edit Row** button.

---

## Integration of CS-MARS and Security Manager

While Cisco Security Manager lets you centrally manage security policies and device settings in large-scale networks, 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. 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 provide additional information about the cross-communication between Security Manager and CS-MARS:

- [NetFlow Event Reporting in CS-MARS, page 21-17](#)
- [Understanding CS-MARS Event Querying, page 21-21](#)
- [Checklist for Integrating CS-MARS with Security Manager, page 21-19](#)

These sections describe how to register CS-MARS servers in Security Manager, and how to view the access-rule and signature event information provided by CS-MARS:

- [Registering CS-MARS Servers in Security Manager, page 21-22](#)
- [Discovering or Changing the CS-MARS Server for a Device, page 6-23](#)
- [About Querying for Access Rule Events, page 21-23](#)
- [About Querying for IPS Signature Events, page 21-27](#)

## NetFlow Event Reporting in CS-MARS

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

Introduced with the launch of the Cisco ASA 5580, NetFlow Security Event Logging utilizes 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. Currently, 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. Therefore, syslog messaging can be disabled to 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.

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.

Syslog ID	Syslog Description	NetFlow Event ID	Extended Event ID
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.
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.

## Considerations When Using CS-MARS Querying

Please be aware of the following when you consider configuring cross-communications between Security Manager and CS-MARS:

- HTTPS is required for communication between the Security Manager server and CS-MARS.
- 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 because of the mismatch between Security Manager and the device.
- If logging is not enabled for an access rule on ASA, PIX and FWSM devices, or if logging is not enabled on IOS routers for access rules, a warning message is displayed, and you can only look up traffic-flow events for those rules.

#### Related Topics

- [Checklist for Integrating CS-MARS with Security Manager, page 21-19](#)
- [Understanding CS-MARS Event Querying, page 21-21](#)
- [Registering CS-MARS Servers in Security Manager, page 21-22](#)

## Checklist for Integrating CS-MARS with Security Manager

If you will be using CS-MARS to provide access-rule and IPS-signature event information to Security Manager users, complete the following tasks to integrate the two applications.

**Table 21-2** Integrating CS-MARS and Security Manager

Task	Description
<b>Add the devices to Security Manager and CS-MARS</b>	See <a href="#">Chapter 6, “Managing the Device Inventory”</a> for information about adding devices to the Security Manager inventory. See the <i>User Guide for Cisco Security MARS</i> or the CS-MARS online Help for information about adding devices to the CS-MARS inventory.  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 6500 switches.)
<b>Register Security Manager with CS-MARS</b>	For information on configuring CS-MARS to communicate with Security Manager, see the <i>User Guide for Cisco Security MARS</i> or the CS-MARS online Help.  Note that you may want to create a CS-MARS user account specifically for linking with Security Manager.
<b>Register CS-MARS controllers with Security Manager</b>	For information on registering CS-MARS controllers with Security Manager, see <a href="#">Registering CS-MARS Servers in Security Manager, page 21-22</a> .  You may want to create a Security Manager user account specifically for linking with CS-MARS; refer to <a href="#">Configuring the Security Manager Server to Communicate with CS-MARS, page 21-20</a> for more information.

Table 21-2 Integrating CS-MARS and Security Manager (Continued)

Task	Description
<b>Link CS-MARS controllers to the devices in Security Manager</b>	You can discover the CS-MARS controller(s) monitoring a particular Security Manager device by clicking <b>Discover CS-MARS</b> on its Device Properties page, as described in <a href="#">Discovering or Changing the CS-MARS Server for a Device</a> , page 6-23.
<b>Look up events as needed</b>	You can right-click an entry in an Access Rules or Signatures table in Security Manager and perform query for related historical and real-time events in CS-MARS. See the following sections for more information: <ul style="list-style-type: none"> <li>• <a href="#">Viewing CS-MARS Events for an Access Rule</a>, page 21-24</li> <li>• <a href="#">Viewing CS-MARS Events for an IPS Signature</a>, page 21-27</li> </ul>

## Configuring the Security Manager Server to Communicate with CS-MARS

To prepare the Security Manager server to be queried by CS-MARS, you may have to take the following actions:

- 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 may not be necessary for authentication purposes.

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 21-22
- [Discovering or Changing the CS-MARS Server for a Device](#), page 6-23

## Understanding CS-MARS Event Querying

Sensors and other network devices can continually forward event information to CS-MARS. These events are stored in the CS-MARS database. Querying for “historical” events from Security Manager lets you view event information stored in the CS-MARS database. You also can navigate from policies in Security Manager to view events as they are forwarded to CS-MARS, in nearly real-time. See [About Real-time and Historical CS-MARS Events, page 21-21](#) for information about the differences between real-time and historical queries.

You can navigate to the Query page of CS-MARS from the Firewall > Access Rules or the IPS > Signatures > Signatures policies in Security Manager, to run an event query based on those specific policy settings. The results of the query let you examine events generated by the access rule or IPS signature, and modify the policy as needed.

You can right-click a signature or an access rule, depending on the type of the device, to set up a real-time event query, or a standard, sessionized (a “historical”) query in CS-MARS. You can then run the query, or save the query criteria to re-use as a report. The results of a query and a report are exactly the same, but saving reports lets you avoid entering the same values every time you want that specific output.

Security Manager requests specific event data by supplying CS-MARS with relevant device details and event-identification information. CS-MARS then creates a query based on the provided information and displays a Query-related page. Real-time queries are run automatically and the results displayed. For historical queries, the Query Criteria window opens; you can either run the query, or save the criteria as a “report” to run at a later time.

Because Security Manager and CS-MARS do not share a common device repository, the query created by Security Manager and sent to CS-MARS includes all the device details (management IP address, host name, domain name, and so on) available in the Security Manager database. CS-MARS compares this information to the device information in its database. Event look-up succeeds only if the relevant devices are recognized by both Security Manager and CS-MARS, and can be reached by CS-MARS using the specified IP address or fully qualified domain name.

### Related Topics

- [Viewing CS-MARS Events for an Access Rule, page 21-24](#)
- [Viewing CS-MARS Events for an IPS Signature, page 21-27](#)

## About Real-time and Historical CS-MARS Events

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.



### Note

---

When you perform an historical event query in Security Manager, syslog messages triggered by connection establishment and tear-down are included.

---

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.

Because sessionization takes time, keeping an event in cache for up to two minutes, the real-time event query can be used to view events right after parsing, providing access to the most current data received. Historical event reports help you identify trends over longer periods of time than is possible with real-time monitoring.

When you choose to 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.

#### Related Topics

- [Understanding CS-MARS Event Querying, page 21-21](#)
- [Viewing CS-MARS Events for an Access Rule, page 21-24](#)
- [Viewing CS-MARS Events for an IPS Signature, page 21-27](#)

## Registering CS-MARS Servers in Security Manager

Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a separate application that monitors devices and collects syslog messages, NetFlow Security Event logs, and other event information. If you use Security Manager to configure firewall access rules and IPS signatures, you can configure CS-MARS to collect information related to those rules. Security Manager users can then directly view messages and events related to specific rules on a device. This integration makes it easy for users to identify and analyze the results of Security Manager rules without having to perform an independent query in CS-MARS.

As part of the process to enable this cross-communication, you must register your CS-MARS controllers with Security Manager. (Refer to the [Checklist for Integrating CS-MARS with Security Manager, page 21-19](#) for information about the other steps.)

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 Server for a Device, page 6-23](#) for more information.)

This procedure explains how to register CS-MARS controllers with Security Manager.

#### Procedure

- 
- Step 1** Choose **Tools > Security Manager Administration** to open the Security Manager Administration window.
- Select **CS-MARS** in the table of contents to display the [CS-MARS Page, page A-3](#).
- 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 A-4](#) 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.
- Step 5** Click **Save** on the CS-MARS page to save your changes.

## About Querying for Access Rule Events

Firewall access 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 entry in the list known as an access-control entry (ACE).

When deciding whether to forward or drop a packet, a device tests the packet against each access rule in the order listed. For the device to generate log entries, the individual access rules must be configured to generate log messages when they are matched.

You can right-click an access rule in the Security Manager table and query CS-MARS for real-time or historical events related to that rule, as follows:

- **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.
- **Rule** – If logging is enabled for the rule (in the [Advanced Dialog Box, page I-8](#)), CS-MARS will record the logged events (assuming it 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.
- **Source** – If you right-click the Source cell in an access rule entry, you also can choose to view real-time or historical events matching the rule's source IP address.
- **Destination** – Similarly, if you right-click the Destination cell in an entry, you can choose to view real-time or historical events matching the rule's destination IP address.

When you query for Rule events from an access rule in Security Manager, keywords are included in the CS-MARS query criteria. These keywords include the ACL ID and the rule's ACE hashcode, if available.

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.

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 (not provided for traffic-flow queries) – ACL name and ACE hashcode, if available, connected by the logical operator OR.

**Note**

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.

**Related Topics**

- [Understanding CS-MARS Event Querying, page 21-21](#)
- [Viewing CS-MARS Events for an Access Rule, page 21-24](#)
- [About Querying for IPS Signature Events, page 21-27](#)

## Viewing CS-MARS Events for an Access Rule

From the Firewall > Access Rules page 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.

If logging is not enabled for a particular access rule, you cannot query for rule-based events, but you can view flow-related events. See [Advanced Dialog Box, page I-8](#) for information about enabling logging for an access rule.

**Note**

When you query for events matching a traffic flow, the report includes events triggered by connection set-up and tear-down, where the rule-based report does not.

The following procedure describes how to look up real-time and historical CS-MARS events related to an access rule in Security Manager.

**Related Topics**

- [About Querying for Access Rule Events, page 21-23](#)
- [Viewing CS-MARS Events for an IPS Signature, page 21-27](#)

## Procedure

**Step 1** Select a security appliance in the Device selector.

**Step 2** Select **Firewall > Access Rules** to display the [Access Rules Page, page I-1](#).

**Step 3** Right-click the desired entry in the access rule table to open the table's shortcut menu.

Note that if you right-click the Source or Destination cell of the table entry, additional source-related or destination-related options will be available in the shortcut menu.

**Step 4** Choose one of the following **Show Events** options from the shortcut menu:

Show Event Option	Description
<b>Realtime &gt; Matching this Flow</b>	<p>To view real-time query results in CS-MARS for events matching this traffic flow (as defined by source and destination IP addresses, protocols, and ports); the results will include connection set-up and tear-down messages.</p> <p>This option is available regardless of whether logging is enabled for the access rule.</p> <p>You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.</p>
<b>Realtime &gt; Matching this Rule</b>	<p>To view real-time query results in CS-MARS for events matching this rule (flow parameters plus Keywords); results begin scrolling within five seconds. Note that this query cannot be run if logging is not enabled for the selected access rule. In this case, you are offered the option of viewing real-time flow results instead.</p> <p>If the selected device does not support hashcodes, a warning is displayed that query results may be inaccurate because of keyword ambiguity; you can proceed with the query, and then edit the query Keyword list and resubmit. ACE hashcodes are supported only on ASA or PIX 7.x and later security appliances.</p> <p>You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.</p>
<b>Realtime &gt; Matching this Source</b> (optional)	<p>To view real-time query results in CS-MARS for events with a source address matching the Source address of this entry. This option is available only when you right-click the Source cell of an entry in the Access Rules table.</p> <p>You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.</p>
<b>Realtime &gt; Matching this Destination</b> (optional)	<p>To view real-time query results in CS-MARS for events with a destination address matching the Destination address of this entry. This option is available only when you right-click the Destination cell of an entry in the Access Rules table.</p> <p>You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.</p>

Show Event Option	Description
<b>Historical &gt; Matching this Flow</b>	<p>Opens the historical query criteria page in CS-MARS with fields populated based on the selected rule's traffic flow (as defined by source and destination IP addresses, protocols, and ports).</p> <p>Edit the rule parameters and query criteria as desired, and click <b>Apply</b> to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.</p> <p>The results will include connection set-up and tear-down messages.</p>
<b>Historical &gt; Matching this Rule</b>	<p>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 <b>Apply</b> to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.</p> <p>Note that a rule-based query cannot be run if logging is not enabled for the selected access rule. In this case, you are offered the option of viewing real-time flow results instead.</p> <p>If the selected device does not support hashcodes, a warning is displayed that query results may be inaccurate because of keyword ambiguity; you can proceed to the CS-MARS query window and edit the Keyword list. ACE hashcodes are supported only on ASA or PIX 7.x and later security appliances.</p>
<b>Historical &gt; Matching this Source</b> (optional)	<p>Opens the historical query criteria page in CS-MARS with fields populated based on the access rule's Source address. Edit the rule parameters and query criteria as desired, and click <b>Apply</b> to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.</p> <p>This option is available only when you right-click the Source cell of an entry in the Access Rules table.</p>
<b>Historical &gt; Matching this Destination</b> (optional)	<p>Opens the historical query criteria page in CS-MARS with fields populated based on the access rule's Destination address. Edit the rule parameters and query criteria as desired, and click <b>Apply</b> to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.</p> <p>This option is available only when you right-click the Destination cell of an entry in the Access Rules table.</p>

**Step 5** If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.

**Step 6** Depending how credentials verification is set up on your system, you may be prompted to log into CS-MARS. See [Registering CS-MARS Servers in Security Manager, page 21-22](#) for more information.

The CS-MARS Query Results or the Query Criteria page opens, depending on whether you are querying for real-time or historical events, with the query fields populated with access-rule details. You can edit the query and save it as a report if you want to run it again later.

## About Querying for IPS Signature Events

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 on the Signatures page in Security Manager and navigate to the CS-MARS Query page to view real-time and historical events.

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 of the CS-MARS query, along with other device information and signature parameters.

**Note**

Events of type `Packet Data` are not displayed in the query results because these events are not triggered by signature rules.

**Related Topics**

- [Understanding CS-MARS Event Querying, page 21-21](#)
- [Viewing CS-MARS Events for an IPS Signature, page 21-27](#)
- [About Querying for Access Rule Events, page 21-23](#)

## Viewing CS-MARS Events for an IPS Signature

From the Signatures policy page in Security Manager, you can select one or more signatures and view related historical or real-time events in CS-MARS.

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.

The following procedure describes how to look up real-time and historical events triggered by an IPS signature.

**Related Topics**

- [About Querying for IPS Signature Events, page 21-27](#)
- [Viewing CS-MARS Events for an Access Rule, page 21-24](#)

**Procedure**

- Step 1** Select an IPS or IOS IPS device in the Device selector.
- Step 2** Select **IPS > Signatures > Signatures** to display the [Signatures Page, page M-1](#).

**Step 3** Right-click the desired entry in the signatures table to open the page's shortcut menu.



**Note** To query for events from multiple signatures, you can select multiple entries and then right-click one of them.

---

**Step 4** Choose one of the following **Show Events** options from the shortcut 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 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.

**Step 5** If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.

**Step 6** Depending how credentials verification is set up on your system, you may be prompted to log into CS-MARS. See [Registering CS-MARS Servers in Security Manager, page 21-22](#) for more information.

The CS-MARS Query Results or the Query Criteria page opens, depending on whether you are querying for real-time or historical events, with the query fields populated with signature details. You can edit the query and save it as a report if you want to run it again later.

---