



CHAPTER 21

Using Monitoring, Troubleshooting, and Diagnostic Tools

High network availability is a requirement for large enterprise and service provider networks. Network managers face increasing challenges to providing high availability, including unscheduled down time, lack of expertise, insufficient tools, complex technologies, business consolidation, and competing markets. Monitoring involves the study of network activities and device status to identify anomalous activities or behavior. Diagnosing and correcting network and system faults (outages and degradations) increases service availability and tools to isolate, analyze, and correct faults are highly imperative. The following topics describe the tools that are available in Security Manager 3.1 to provide integrated network monitoring services and diagnostic capabilities for troubleshooting significant events in your network and resolution:

- [Device Managers, page 21-2](#)
- [Device Connectivity Test, page 21-15](#)
- [Performance Monitor \(Status Provider\), page 21-15](#)
- [IPS Event Viewer, page 21-31](#)
- [Security Manager Access Rule Lookup from Device Manager Syslog, page 21-42](#)

Device Managers

In Security Manager 3.0.1 and earlier, you cannot start device managers for devices that are managed by Security Manager, with the exception of Catalyst 6500/7600 Device Manager (DM 6500/7600). With Security Manager 3.1, you can start device managers for all supported devices, such as PIX security appliances, Firewall Services Module (FWSM), IPS sensors, IOS routers, and Adaptive Security Appliance (ASA) devices. Device managers provide several monitoring and diagnostic features that enable you to get information regarding the services running on the device and a snapshot of the overall health of the system. By starting device managers from Security Manager, you eliminate the need to open an HTTPS connection between your client system and the device you want to monitor.

The Security Manager server is shipped with device manager images for the supported devices. When the Security Manager server receives a request to start a device manager, the corresponding device manager image is downloaded to the Security Manager client. The default location for the device manager images is C:\Program Files\Cisco Systems\Cisco Security Manager Client\cache. The device manager images are uninstalled when you uninstall the Security Manager client on your client system.

**Note**

When you use a device manager that you started from Security Manager, you can only view the existing device configuration. If you perform configuration changes from the device manager, and save the changes to apply them to the running configuration of the device, an error message is displayed stating that the device manager started from Security Manager does not allow you to perform configuration changes on the device.

Although you can modify device configurations using the device manager running on the device, we recommend that you do not make changes to a device configuration outside of Security Manager (an out-of-band change) if you are adding the device to the inventory to be managed by Security Manager.

The following topics describe the device managers that you can start from Security Manager:

- [IDM, page 21-3](#)
- [PDM, page 21-4](#)

- [ASDM, page 21-5](#)
- [SDM, page 21-6](#)

IDM

The Cisco Intrusion Prevention System (IPS) Sensor software is an inline, network-based solution, that identifies, classifies, and stops malicious traffic, including worms, spyware/adware, network viruses, and application abuse, before they affect business continuity. IPS sensors analyze network packets and flows to determine whether their contents appear to indicate a network intrusion. Additionally, the IPS solution, in combination with IPS Sensor software, works with other network security resources to provide proactive protection of your network.

Intrusion Prevention System Device Manager (IDM) is an application that enables you to configure and manage your IPS sensors. The web server for IDM resides on the sensor. Security Manager provides the ability to start IDM without the need for IDM to be installed on your IPS sensor. IDM started from Security Manager does not depend on the type of browser. Using IDM, you can monitor whether sensors that are initialized and configured to be managed by IDM can be reached and are functioning properly. When an IPS sensor detects an unauthorized network activity, the alarm generated can be viewed from IDM.



Note

The IDM user interface consists of the File and Help menus. There are Configuration and Monitoring buttons in IDM 5.0 and 5.1 whereas IDM 6.0 contains an additional button, Home. IDM constantly retrieves status information to keep the Home window updated with the device details, alert summary, and sensor resource and interface status.

From an IDM started from Security Manager client, you can click the **Monitoring** button and navigate to the menus in the left-hand pane to configure monitoring. You can use the Monitoring menus to edit the settings that enable you to monitor sensor health.

When you access the online help for IDM 5.1, the Enter Network Password dialog box pops up after you click Yes in the Security Alert dialog box. Enter your username and password and click OK. This behavior is different from the method

of accessing online help for other versions of IDMs in which only the security certificate alert appears and you are not prompted to enter credentials to display online help.

See [IDM product documentation](#) for more information.

Related Topics

- [Device Managers, page 21-2](#)
- [Understanding Communication, page 21-7](#)
- [Starting Device Managers, page 21-7](#)

PDM

PIX Device Manager (PDM) software provides secure administration of FWSM and PIX Firewalls. Security Manager provides the ability to start PDM without the need for PDM to be installed on your PIX Firewall or FWSM. PDM started from Security Manager does not depend on the type of browser and uses the Java plug-in shipped with Security Manager. PDM manages FWSM Releases 1.1, 2.3 and 2.2 when it runs in single or multiple context modes, and PIX OS versions 6.0 through 6.3.

PDM provides you with a graphical user interface to the firewall and FWSM to administer it. PDM is also compatible with the firewall and FWSM CLI and includes a tool for using standard CLI commands within PDM. With PDM, you can graph many aspects of the firewall and FWSM, including system activity such as CPU and memory utilization, and performance statistics for xlates, connections, AAA, fixups, URL filtering and TCP Intercept. You can also print or export the graphs. Additionally, using PDM, you can monitor DHCP client lease information, interface statistics, Telnet and SSH sessions, current PDM sessions to the firewall, syslog messages based on their level of severity, and VPN tunnels.

The PDM home page lets you view at a glance important information about your firewall such as the status of your interfaces, the version you are running, licensing information, and performance. Many of the details available on the PDM home page are available elsewhere in PDM, but this is a useful and quick way to see how your firewall is running. All information on the home page is updated every ten seconds, except for the Device Information.

See [PDM product documentation](#) for more information.

Related Topics

- [Device Managers, page 21-2](#)
- [Understanding Communication, page 21-7](#)
- [Starting Device Managers, page 21-7](#)

ASDM

Cisco Adaptive Security Device Manager (ASDM) provides security management and monitoring through a web-based management interface. Bundled with ASA 5500 Series Adaptive Security Appliances, PIX Security Appliances, and FWSM, ASDM integrates an array of robust security services to prevent unauthorized administrative access to a device. Security Manager provides the ability to start ASDM without the need for ASDM to be installed on your device. ASDM started from Security Manager does not depend on a type of browser and uses the same Java plug-in that is shipped with Security Manager.

ASDM offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the home page. You can view detailed device status information, including blocks used and free, current memory utilization, and CPU utilization. ASDM also tracks real-time session and performance monitoring data for connections, address translations, and AAA transactions on a per-second basis. Connection graphs enable you to stay fully informed of your network connections and activities. ASDM provides 16 different graphs to display potentially malicious activity, real-time monitoring of bandwidth usage for each interface on the security appliance, and VPN statistics and connection graphs. By running separate instances of ASDM, you can connect to multiple security appliances from a single workstation.

The ASDM home page includes a dynamic dashboard that provides a complete system overview and device health statistics at a glance. You can view important information about your security appliance, such as the status of your interfaces, CPU and memory usage details, number of connected IKE and IPsec tunnels, the version you are running, device information, UDP and TCP connections per second, real-time syslog viewer and traffic throughput. Many of the details available on the ASDM home page are available elsewhere in ASDM, but this is a useful and quick way to see how your security appliance is running. Status information on the Home page is updated every ten seconds.

See [ASDM product documentation](#) for more information.

Related Topics

- [Device Managers, page 21-2](#)
- [Understanding Communication, page 21-7](#)
- [Starting Device Managers, page 21-7](#)

SDM

Cisco Router and Security Device Manager (SDM) is a tool that can be used to proactively manage Cisco IOS software-based router resources and security before they affect mission-critical applications on the network. Security Manager provides the ability to start SDM without the need for SDM to be installed on your router. SDM started from Security Manager does not depend on the type of browser. 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.

The SDM home page displays system and configuration overview information about your router hardware and software, such as the running configuration, interface-specific firewall policies, and number of static and dynamic routes. The home page provides for faster and easier monitoring of security configurations.

The home page also provides a quick snapshot of detailed VPN status, such as the number of active VPN connections, the name of an interface with a configured VPN connection, the type of VPN connection configured on the interface, and the name of the IPsec policy associated with the VPN connection.

See [SDM product documentation](#) for more information.

Related Topics

- [Device Managers, page 21-2](#)
- [Understanding Communication, page 21-7](#)
- [Starting Device Managers, page 21-7](#)

Understanding Communication

Security Manager client intercepts all HTTPS requests made by device managers and sends them to the Security Manager server. The server processes the requests redirected by the client by obtaining information from the device or sending data such as the device manager image to the client. This communication between the client and server is transparent to the device manager, and appears as though there is a direct connection between the device manager and the device. Because the Security Manager client intercepts all requests from the device manager, you do not need to enable SSL on all Security Manager clients for secure access between the client and the server and between the device manager and Security Manager.

When a device manager is started from Security Manager, the Security Manager client starts the correct device manager image for the selected device. If the device manager image is not available in the client cache directory, the image is obtained from the Security Manager server. The Security Manager client starts only one instance of device manager per device and closes the device manager window when you exit the Security Manager client or the idle session timeout period is exceeded.

Related Topics

- [Device Managers, page 21-2](#)
- [Starting Device Managers, page 21-7](#)
- [Device OS Version Interoperability with Device Managers, page 21-13](#)

Starting Device Managers

You can start device managers for all devices (both static and dynamic IP addresses) that are supported by Security Manager. Device managers can be started on all versions of Windows that are supported by Security Manager. The device manager opens in a separate window and you can switch between the Security Manager client and device manager windows at any time. If the device manager window for a device is not active or has been minimized, an error message is displayed when you attempt to start the device manager for the same device. You can either choose to close the previous instance of device manager and start a new window, or cancel the operation to start a fresh device manager instance and activate the device manager window that was started before. The credentials that you supplied while adding the device to Security Manager

inventory are reused to start the device manager. If you did not enter the device credentials while adding the device, an error message is displayed when you start the device manager stating that the device credential information for logging in to the device must be entered.

Keep in mind the following guidelines when working with device managers started from Security Manager:

- Security Manager is shipped with device manager images and does not use the device manager image installed on the device to start a device manager.
- 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 clients.
- You can start device managers for multiple devices at the same time from the same Security Manager client.
- You can start only one device manager per device per Security Manager client.
- You can start multiple device managers for the same device at the same time from different Security Manager clients systems.
- You can start a device manager from Security Manager even if the device manager is not installed on the device.
- The security appliance and FWSM allow a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances divided between all contexts for security appliance and 80 ASDM sessions between all contexts for FWSM. To display a list of active ASDM sessions and their associated session IDs, use the **show asdm sessions** command in privileged EXEC mode. ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts.

The maximum number of persistent HTTPS connections that can be established with the security appliance is limited by the system limit for your device model. An error message is displayed if you attempt to exceed this limit. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

- PDM allows multiple PCs or workstations to each have one browser session open with the same firewall. A single firewall can support up to 16 concurrent PDM sessions. Only one session per browser per PC or workstation is supported for a particular firewall. The FWSM allows up to 32 PDM sessions for the entire module, and it allows a maximum of 5 concurrent HTTPS connections per context, which can be configurable.
- The number of concurrent IDM sessions is limited based on the IPS platform. IDS-4210, IDS-4215, and NM-CIDS are limited to three concurrent sessions. All other platforms allow ten concurrent sessions.
- If the device has a newer OS version, which is not supported by Security Manager, the most recent version of device manager that supports the OS version on the device is started. If no such version of device manager exists on the client, an error message is displayed when you start the device manager for such a device.
- The device manager started from Security Manager for a Cisco IOS router supports the most recent Cisco IOS software release, regardless of whether the device manager running on the router supports the most recent version of Cisco IOS software or not.
- You need to modify the Cisco Security Agent or any other anti-virus and network firewall software policies on the Security Manager client system to allow the device manager (xdm-launcher.exe) to be cross-launched. Else, the security agent installed on your client system might terminate the execution of the xdm-launcher.exe file when you attempt to start device manager.
- Starting multiple device managers might impact the Security Manager server and client performance. Memory and performance impact on the client is proportional to the number of device managers that are started. Increased number of requests to start device managers or retrieve current information from the device can have an adverse impact on the server performance.
- Device managers started from Security Manager provide read-only view. The home pages of device managers provide a bird's eye view of device health statistics and vital system information. In addition to the dashboard view capabilities on the home page, you can navigate to the other menus and view detailed information on various device configuration parameters.
- Device managers can be started for FWSM blades and ASA devices running in transparent mode (Layer 2 firewall) or routed mode (Layer 3 firewall) and supporting single security context or multiple security context. For FWSM

and ASA devices in which multiple independent virtual firewall security contexts exist, you must define a unique management IP address for each security context to start the device manager.

- The credentials for the device that you entered using the Device Credentials page when you added the device to Security Manager are used to start the device manager for that device; you need not reenter the credentials. However, if you have not entered the device credentials during device addition to the Security Manager inventory, an error message indicates that the device credentials are not available when you start the device manager. Double-click the device in the Device selector, then click **Credentials** from the Device Properties page to add device credential information to the Security Manager database.
- You must enable HTTPS server on the devices so that the Security Manager client can intercept all requests from device managers and redirect them to the server. See the relevant product documentation for information on how to enable HTTPS server on the devices.
- The preferences that you set to change the behavior of some device manager functions in the read-only view are retained across sessions. For example, if you choose not to display the confirmation prompt when you try to exit the device manager window, that setting applies to all future instances of the device manager.
- You can access the command line interface (CLI) on the device from the Tools menu of device manager started from Security Manager and run several **show** commands to help you view pertinent information about device configuration parameters. Only **show** commands can be run from the Tools menu and you cannot execute other commands on the device from device manager.
- From an IDM started from Security Manager client, you can click the **Monitoring** button and navigate to the menus in the left-hand pane to configure monitoring. You can use the Monitoring menus to edit the settings that enable you to monitor sensor health.
- When you exit the Security Manager client, all device manager windows are closed.

This procedure describes how to start a device manager for a device added to the Security Manager inventory.

Before You Begin

- If an instance of the device manager is already running on your client system, an error message is displayed when you try to start the device manager again for the same device. If you get this error message, you are prompted to confirm whether you want to close the device manager window that was previously started and start it afresh or terminate the start operation. Click **OK** to close the previous instance of device manager and start a new window.
- Because Security Manager cannot determine the management interface and, therefore, the management IP address when you add a device from a configuration file, the hostname in the configuration file is used as the DNS hostname. If the hostname is missing in the CLI of the configuration file, the configuration filename is used as the DNS hostname. During live device discovery, the DNS hostname in the Device Properties page is not updated with the hostname configured on the device. Therefore, if the DNS hostname that appears on the Device Properties page is not the same as the hostname that you configured on the device, the device manager fails to start.
- Ensure that you have valid and complete configurations for the primary credentials and HTTP connection-related configurations by editing the device credentials information from the Device Properties page.
- If Security Manager cannot reach the device, an error message is displayed and the device manager fails to start. Configure device communication settings, such as device identity, the operating system running on the device, and device communication settings using the Device Properties page to establish a connection between Security Manager and the device.
- If Security Manager cannot reach the device and the device credentials are also not specified, an error message is displayed stating that the credential information for the device is not available when Security Manager checks the device properties before attempting to start the device manager.
- If SSL is not enabled on the device for secure access between the Security Manager server and the device, an error message is displayed when you try to start the device manager. Ensure SSL is enabled on the device so that communication between the Security Manager and device is encrypted. See the relevant product documentation for the command you must configure to enable SSL on the device.



Note DES encryption is not supported on Common Services 3.0 and later. Please make sure that all PIX Firewalls and Adaptive Security Appliances that you intend to manage with Cisco Security Manager have a 3DES/AES license.

Procedure

Step 1 Click the **Device View** button on the toolbar. The Devices page appears.

Step 2 In Device view, select a device from the Device selector, then do one of the following:

- From the Device selector, right-click a device to display menu options, then select **Device Manager**.
- Select **Tools > Device Manager**.

A warning message states that the device manager started from Security Manager does not allow you to perform configuration changes on the device and asks if you want to continue.



Tip To prevent this warning message from appearing in the future for any device, select the **Do not show this again** check box before continuing.

Step 3 To continue, click **Yes**.



Note When you start a device manager from Security Manager, the xdm-launcher.exe application, which is the device manager image, is run. If you had set the Cisco Security Agent (CSA) security level to medium or high on your server system, CSA displays a popup window, which indicates that a problem is detected, prompting you to confirm whether you want to allow xdm-launcher.exe to be started. You can either click **Yes** to allow the xdm-launcher.exe process to run whenever you are prompted to confirm, or modify the CSA policies on the Security Manager client system to allow xdm-launcher.exe to be run always.

If you have configured the CSA policies to prevent the execution of the xdm-launcher.exe process, the icon in the system tray (the red flag) will

wave to indicate that CSA has a message for you when you start device manager. To read the message, double-click the CSA icon (the red flag in the Windows system tray) to open the CSA utility. The Messages tab displays by default. CSA considers `xdm.launcher.exe` as an untrusted application and places this information in the Untrusted Applications edit box. To remove the program executable from the list of untrusted applications, from the Untrusted Applications window of the CSA utility, select the `<installation_location>\Cisco Security Manager Client\cache\xdm.launcher.exe` entry in the edit box, where `<installation_location>` is the drive and directory in which you installed Security Manager client and press the **Delete** key. The restriction on the device manager application is removed and the device manager allowed to be started from Security Manager.

A progress bar indicates the progress of the device manager start and displays what percentage of the launch has been completed. The device manager home page is displayed when the start operation is complete.

Related Topics

- [Device Managers, page 21-2](#)
- [Understanding Communication, page 21-7](#)
- [Device OS Version Interoperability with Device Managers, page 21-13](#)

Device OS Version Interoperability with Device Managers

Each version of the device manager image is compatible with specific versions of software running on the device. The most recent version of device manager supported for the software version running on the device is started from Security Manager, regardless of the device manager version installed on the device. For example, if SDM 2.2 is installed on a router running Cisco IOS 12.3 release, when you start the device manager for this router from Security Manager, SDM 2.3.2, which is the most recent version of SDM that supports the current and earlier Cisco IOS releases, is started. The version of device manager installed on the device is not taken into consideration. Only the most recent version of device manager is started for all devices.

**Note**

For more information on the minimum hardware requirements for the device manager software, see the relevant device manager product documentation.

Table 21-1 lists the device manager version supported for the software version running on the device when you start the device manager from Security Manager.

Table 21-1 Supported Device Manager Versions and Device OS Versions

Device Manager	Device Manager OS Version	Device OS Version
ASDM	5.0(1)F	FWSM 3.1 ¹
	5.2(2)	ASA 7.2 ¹
	5.1(2)	ASA 7.1 ¹ , PIX 7.1
	5.0(4)	ASA 7.0 ¹ , PIX 7.0
PDM	4.1(3)	FWSM 2.2, 2.3 ¹
	3.0(4)	PIX 6.3
	2.1(1)	PIX 6.2, FWSM 1.1 ¹
	1.1(2)	PIX 6.0, 6.1
IDM	5.1	IPS 5.0(x), IPS 5.1(x)
	6.0	IPS 6.0(x)
SDM	2.3.4	Most recent and previous releases of Cisco IOS software running on your Cisco router.

1. Device managers can be started for FWSM blades and ASA devices running in transparent mode (Layer 2 firewall) or routed mode (Layer 3 firewall) and supporting single security context or multiple security context.

Related Topics

- [Device Managers, page 21-2](#)
- [Starting Device Managers, page 21-7](#)
- [Device OS Version Interoperability with Device Managers, page 21-13](#)

Device Connectivity Test

In Cisco Security Manager 3.0.1 and earlier, you cannot validate whether a device that is added to the Security Manager inventory can be reached. Although Security Manager validates the data you entered, it does not validate whether the data you entered will allow you to contact the device. In release 3.1, you can verify whether Security Manager can contact the device when you are adding the device. For more information on device connectivity test, see [Working with Device Connectivity Test, page 5-45](#).

Related Topics

- [Working with Device Connectivity Test, page 5-45](#)

Performance Monitor (Status Provider)

Effective network management requires the fastest possible identification and resolution of events that occur on mission-critical systems. As a result, the need to monitor and troubleshoot the health and performance of enterprise network security services has become very essential. Security Manager 3.0.1 and earlier enabled you to centrally administer security policies and device settings for either small or large scale networks. However, any errors generated by deploying configurations containing these policies to devices or while discovering policies from devices were not easy to rectify. In some cases, a deployment or discovery error could have been caused by device connectivity or network problems rather than an incorrect policy configuration.

Security Manager 3.1 enables you to configure status providers that collect information about the status of various events from external sources or status providers, such as Performance Monitor, and from internal sources, such as deployment. As a status provider, Performance Monitor collects the status of events, such as VPN tunnel up/down status, device reachability, and CPU usage threshold, and reports them to Security Manager. You can use the Inventory Status window in the Security Manager GUI to view the events reported by status providers. Performance Monitor is a browser-based tool that monitors and troubleshoots the health and performance of services that contribute to network security. It helps you to isolate, analyze, and troubleshoot events in your network as they occur, so that you can increase service availability.

Performance Monitor, which is an external status provider, must be registered with Security Manager and needs to be authenticated by Security Manager to send status on events it is monitoring. Security Manager authenticates Performance Monitor by comparing the username and password with the account information stored in the CiscoWorks or Cisco Secure Access Control Server (ACS) database, depending on which you established at installation as your AAA provider. After the authentication of your credentials, Security Manager begins to receive the status of events. Security Manager uses SSL to establish a secure communication with Performance Monitor. You must add a device to both the Security Manager inventory and Performance Monitor for its status to be collected and displayed by the Security Manager client. If the device is deleted from Performance Monitor but is still available in Security Manager, or if you excluded the device from being polled by Performance Monitor, the health and performance of the device is not displayed by Security Manager.

Related Topics

- [Understanding Performance Monitor as a Status Provider, page 21-16](#)
- [Configuring Performance Monitor as a Status Provider, page 21-17](#)
- [Understanding the Events to be Monitored, page 21-18](#)

Understanding Performance Monitor as a Status Provider

Security Manager polls data from external status providers, such as Performance Monitor, at an interval of five minutes by default. When a new external status provider is added, Security Manager begins polling and displays events from that provider. When a status provider is deleted from Security Manager, events from that provider are not displayed and polling of that provider is stopped. When the Security Manager server is restarted, the last event statuses that were obtained from deployment and Performance Monitor are displayed until the next polling cycle.

Security Manager overwrites the older events with the most recent events reported by status providers. Most recent events refer to events that were reported most recently by the providers for each event type. In other words, Security Manager does not accumulate the events reported by status providers at different points in time. As an example of two most recent events that will be persisted for Device1, assume that Performance Monitor logs a “DEVICE” event type with “critical” severity level, an “INTERFACE” event type with “warning” severity level at

12:00 noon, and no events of the same type have occurred since then until the time you view the event statuses in the Inventory Status window. In this case, both events would be displayed. As an example of one most recent event that will be persisted for Device 1, assume that Performance Monitor logs a “DEVICE” event type with “warning” severity level at 1:00 p.m. and another “DEVICE” event type with “critical” severity level at 2:00 p.m. When you view the Inventory Status window at say, 2:00 p.m., the event that occurred at 2:00 p.m. would only be retained and displayed.

Whenever Cisco Security Manager Daemon Manager is started or restarted, or the connection is restored with Performance Monitor after a network outage, Security Manager sends a list of devices, whose status needs to be monitored, to Performance Monitor. Security Manager also notifies Performance Monitor when a new device is added to the inventory or an existing device is deleted from the inventory. Security Manager also polls Performance Monitor for incremental changes in status at other times.

Related Topics

- [Performance Monitor \(Status Provider\), page 21-15](#)
- [Configuring Performance Monitor as a Status Provider, page 21-17](#)
- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Services and Platforms for Monitoring and Reports, page 21-25](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Working with Event Thresholds, page 21-28](#)

Configuring Performance Monitor as a Status Provider

The Status Provider page enables you to select the status providers that you want to send information to the Security Manager server. Depending on the status providers you choose, Security Manager polls the appropriate sources and modifies the display of events in the Inventory Status window.

You can add more than one Performance Monitor as a status provider and view status messages from all of them at the same time. Additionally, you can configure the same status provider to send event details to multiple Security Manager servers. You can also view information from the same Performance Monitor on multiple Security Manager clients.

For more information on how to configure Performance Monitor as a status provider to send event details to Security Manager, see [Working with Status Providers](#), page 2-94.

Related Topics

- [Understanding Performance Monitor as a Status Provider](#), page 21-16
- [Configuring Performance Monitor as a Status Provider](#), page 21-17
- [Understanding the Events to be Monitored](#), page 21-18
- [Supported Services and Platforms for Monitoring and Reports](#), page 21-25
- [Supported Event Types for Each Service Type](#), page 21-27
- [Working with Event Thresholds](#), page 21-28

Understanding the Events to be Monitored

From the Inventory Status window, select a device in the upper pane and click the Status tab in the lower pane to view the list of Performance Monitors configured as status providers. You can click the arrow to expand or collapse the events reported by each status provider. Similarly, you can expand and collapse the event details by clicking the arrow next to the event name. The status of each event (whether it is normal or an abnormal condition has occurred) is displayed next to the event name. [Table 21-2](#) describes the fields displayed for each event.

Table 21-2 *Event Status Elements*

Element	Description
Timestamp	Displays the most recent time at which Security Manager polling recorded the problem.
Description	Displays a description of the problem condition.
Recommended Action	Information about how the warning, error, or failure might be corrected.

Performance Monitor collects the status of events, such as VPN tunnel up/down status, device reachability, and CPU usage threshold, and reports them to Security Manager. An event is a notification that a managed device or component has an abnormal condition. Multiple events can occur simultaneously on a single

monitored device or service module. Using Performance Monitor, you can configure a threshold for an event or use the default threshold. For more information on how to configure and enable thresholds to generate performance or failure events of any priority, see [Working with Event Thresholds, page 21-28](#). The events in which a monitored component or service exceeded acceptable thresholds are displayed. Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL. For more information on the service types supported for different device platforms, see [Supported Services and Platforms for Monitoring and Reports, page 21-25](#). The following sections describe the events whose statuses are reported by Performance Monitor to Security Manager:

- [Device Reachability, page 21-19](#)
- [VPN Tunnel Status, page 21-22](#)
- [CPU Usage Threshold, page 21-23](#)

Device Reachability

You must add a device to both the Security Manager inventory and Performance Monitor for its status to be recorded in the Inventory Status window. Security Manager does not display events from devices that are added only to Performance Monitor. The device that you want to monitor must be a device type supported by both Security Manager 3.1 and Performance Monitor 3.1. Using Performance Monitor, you cannot add, import, or validate any unsupported device type, any device when the MCP process has stopped, any device that uses a dynamic IP address or lacks configured SNMP values, and a VPN 3000 Series concentrator, unless you specify the correct SNMP and XML credentials, HTTPS is enabled, and the VPN 3000 Concentrator Series Manager is running.

You must set up devices by configuring the bootstrapping devices so Performance Monitor can validate, poll, and monitor them. Performance Monitor enables you to import or manually enter the IP addresses, hostnames, and read-only community strings for supported devices in your network. You can import device attributes from a comma-separated value (CSV) file or from the Device Credentials Repository (DCR) on a Common Services-based server, or you can add device attributes manually. You can also create device groups to interact with multiple devices in a single operation. A device group is a named entity that can contain devices, other groups, or a combination of devices and groups.

After adding a device to Performance Monitor, you can validate a device of any kind to confirm that it exists and is reachable, has the required features and interfaces enabled, has the correct credentials, uses a static (non-dynamic) IP address, and has configured SNMP values. During device validation, Performance Monitor sets all validated devices to a managed state by default meaning that polling is enabled. If you choose to move a device to an unmanaged state, you must move it back to the managed state manually before you can monitor its health or performance. By default, device validation occurs once every day, at midnight. It also occurs at other times and intervals that you specify. You can perform an immediate, one-time validation at any time. For more information on how to add, validate, and manage devices, see *User Guide for Cisco Performance Monitor 3.1*.

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, a device must have an IP address. For example, you can use multicontext mode to partition a single firewall into multiple virtual devices, known as security contexts. You can add and manage contexts in the system configuration. The system configuration identifies basic firewall settings, but does not include any network interfaces or network settings for itself, rather, it uses a context that is designated as the admin context.

The admin context is just like any other security context, except that a user who logs in to the admin context has administrative rights over the system and all of the other contexts. In Performance Monitor, you import only the admin context from a device when you want to monitor every configured context on a physical device. Similarly, when you delete an admin context in Performance Monitor, you simultaneously delete the record that Performance Monitor maintains for every context on the relevant physical device.

Performance Monitor reports information about only those validated devices for which monitoring is enabled. Performance Monitor enables monitoring after a successful device validation; thus, it polls the device in following polling cycles. If you decide to exclude a device from polling, you can disable monitoring for it. Later, at your discretion, you can reenable monitoring manually.

[Table 21-3](#) describes the different management protocols that Performance Monitor uses to test device connectivity, depending on the device platform.

Table 21-3 *Management Protocols Supported for Device Platforms*

Device Platform	Management Protocols
Cisco IOS VPN Routers	SNMP, HTTPS for some of the show commands, and VPN-related SNMP traps.
Adaptive Security Appliances 5500 Series	SNMP and HTTPS for some of the show commands and some syslogs.
Catalyst 6500 Series Switches with Content-switching Services Modules	SNMP and content-switching module-related SNMP traps.
Catalyst 6500 Series Switches with Firewall Services Modules	SNMP and HTTPS for some of the show commands and some syslogs.
Catalyst 6500 Series Switches with SSL Services Modules	SSH for show commands.
Catalyst 6500 Series Switches with VPNSMs	SNMP, HTTPS for some of the show commands, and VPN-related SNMP traps
PIX Security Appliances (known commonly as PIX Firewalls)	SNMP, HTTPS for some of the show commands and some syslogs.
VPN 3000 Concentrator Series	SNMP, HTTPS, XML interface (if the device is in a cluster), syslogs, and SNMP traps.

After you update the list of devices to be monitored, Performance Monitor polls reachable devices for their current status to compare device status information to performance and failure thresholds, generate performance and failure events, send event notifications, when appropriate, and update the values in tables and graphs. Security Manager obtains and displays a snapshot of the most recent device reachability status in the Inventory Status window during the next polling cycle. For a categorization of the device reachability, VPN tunnel status, and CPU usage event types by service type, see [Table 21-6](#).

Related Topics

- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Services and Platforms for Monitoring and Reports, page 21-25](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Working with Event Thresholds, page 21-28](#)
- [VPN Tunnel Status, page 21-22](#)
- [CPU Usage Threshold, page 21-23](#)

VPN Tunnel Status

Performance Monitor enables you to determine whether a VPN Tunnel is up or down. Whenever a VPN Tunnel is not functioning, an event is logged in the Event Browser window in the Performance Monitor GUI. A tunnel is considered as down when an IPsec security association (SA) is not present. Performance Monitor tracks the IPsec SAs and displays the event status. Internet Key Exchange (IKE) is the facilitator and manager of IPsec-based communications. It is a hybrid protocol used to authenticate IPsec peers, negotiate and distribute encryption keys, and automatically establish IPsec security associations (SAs). IKE protocol lets two hosts agree on how to build an IPsec SA. Each IKE negotiation is divided into a Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects IKE negotiation messages. Phase 2 creates the tunnel that protects data. With IKE keepalive, tunnel peers exchange messages that demonstrate they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals, and any disruption in that interval results in the creation of a new tunnel, using a backup device. Devices that rely on IKE keepalive for resiliency transmit their keepalive messages regardless of whether they are exchanging other information. These keepalive messages can therefore create a small but additional demand on your network.

Both IPsec SAs and IKE SAs can have timeout values. The absence of these SAs does not necessarily indicate a problem with IPsec tunnel. But in majority of site-to-site VPNs, both IPsec SAs and IKE SAs need to be present for all the interesting traffic.

You must define parameters for each of the available authentication methods so that IKE and IPsec can use your IKE policies successfully. For preshared key, you can either enter a key manually, or have Security Manager automatically generate a key for each hub-spoke communication session. When using preshared keys for authentication, you can use main mode or aggressive mode for negotiating key

information and setting up IKE SAs. Security Manager mirrors the spoke's preshared key and configures it on its assigned hub, so that the key on the spoke and hub are the same.

With IPsec, crypto ACLs define what traffic should be protected between two IPsec peers. Traffic might be selected based on source and destination address. The crypto ACLs used for IPsec are used only to determine which traffic should be protected by IPsec, not which traffic should be blocked or permitted through the interface. ACLs are applied to interfaces by way of crypto map sets. Each tunnel policy you create with Security Manager is translated into a crypto map entry that includes an ACL. A crypto map set can contain multiple entries, each with a different ACL. The crypto map entries are searched in order and the router tries to match the packet to the ACL specified in each entry.

When some packets to be encrypted are encountered by the VPN device, it uses the symmetrical keys derived in the IKE SA establishment for encryption of data. The interesting traffic is specified by a crypto ACL as in GRE and standard IPsec VPNs. In DMVPNs, the crypto ACL is derived automatically. The pair of SAs called as IPsec SAs are created for data encryption.

Based on the threshold you configure for the site-to-site VPN tunnel status event type, Security Manager polls Performance Monitor at the preconfigured interval and displays the status in the Inventory Status window. For a categorization of the device reachability, VPN tunnel status, and CPU usage event types by service type, see [Table 21-6](#).

Related Topics

- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Services and Platforms for Monitoring and Reports, page 21-25](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Working with Event Thresholds, page 21-28](#)
- [Device Reachability, page 21-19](#)
- [CPU Usage Threshold, page 21-23](#)

CPU Usage Threshold

Performance Monitor enables you to track and analyze system CPU utilization. Commonly, high CPU utilization is caused by a security issue, such as a worm or virus operating in your network. This is especially likely to be the cause if there

have not been recent changes to the network. Usually, a configuration change, such as adding additional lines to your access lists, can mitigate the effects of this problem. Although debugging can also be of great help in troubleshooting high CPU utilization in processes, it should be carried out with extreme caution because it may raise the CPU utilization even more. Cisco software-based routers use software in order to process and route packets. CPU utilization on a Cisco router tends to increase as the router performs more packet processing and routing. Catalyst 6500/6000 switches do not use the CPU in the same way. These switches make forwarding decisions in hardware, not in software. Therefore, when the switches make the forwarding or switching decision for most frames that pass through the switch, the process does not involve the supervisor engine CPU.

Throttles are a good indication of an overloaded router. They show the number of times the receiver on the port has been disabled, possibly due to buffer or processor overload. Together with high CPU utilization on an interrupt level, throttles indicate that the router is overloaded with traffic. Unusual activity related to a process could also load the CPU and result in an error message in the log. Therefore, the output of the **show logging exec** command should be checked first for any errors related to the process which consumes lots of CPU cycles. When the TCP timer process uses a lot of CPU resources, there are too many TCP connection endpoints. This can happen in data-link switching (DLSw) environments with many peers, or in other environments where many TCP sessions are simultaneously opened on the router. High CPU utilization in the Address Resolution Protocol (ARP) Input process occurs if the router has to originate an excessive number of ARP requests.

High CPU utilization also can result from the merging of two or more VLANs due to improper cabling. Also, if STP is disabled on those ports where the VLAN merger happens, high CPU utilization can occur. The Exec process in Cisco IOS Software is responsible for communication on the TTY lines (console, auxiliary, asynchronous) of the router. The Virtual Exec process is responsible for the VTY lines (Telnet sessions). The Exec and Virtual Exec processes are medium priority processes, so if there are other processes that have a higher priority (High or Critical), the higher priority processes get the CPU resources. If there is a lot of data transferred through these sessions, the CPU utilization for the Exec process increases. High CPU utilization on an interrupt level is primarily caused by packets handled on interrupt level. Interrupts are generated any time a character is output from the console or auxiliary ports of a router. Universal Asynchronous Receiver/Transmitters (UARTs) are slow compared to the processing speed of the

router, so it is unlikely, though possible, that console or auxiliary interrupts can cause a high CPU utilization on the router (unless the router has a large number of tty lines in use).

Based on the threshold you configure for the CPU usage event type associated with a particular service, Security Manager polls Performance Monitor at the preconfigured interval and displays the status in the Inventory Status window. For a categorization of the device reachability, VPN tunnel status, and CPU usage event types by service type, see [Table 21-6](#).

Related Topics

- [Understanding the Events to be Monitored](#), page 21-18
- [Supported Services and Platforms for Monitoring and Reports](#), page 21-25
- [Supported Event Types for Each Service Type](#), page 21-27
- [Working with Event Thresholds](#), page 21-28
- [Device Reachability](#), page 21-19
- [VPN Tunnel Status](#), page 21-22

Supported Services and Platforms for Monitoring and Reports

See [Table 21-4](#) to understand which services this Performance Monitor release can monitor, and can issue reports for, on each supported Cisco platform.

Table 21-4 *Supported Services and Platforms for Monitoring*

Platform ^{1, 2}	Monitored Service Type ^{3, 4}							
	VPN				Firewall		Other	
	DMVPN	Easy VPN	Remote Access	Site-to-Site	Firewall	Multicontext	Load Balancing	SSL
Adaptive Security Appliances 5500 Series	NA	✓	✓	✓	✓	✓	NA	NA

Table 21-4 Supported Services and Platforms for Monitoring (continued)

Platform ^{1, 2}		Monitored Service Type ^{3, 4}							
		VPN				Firewall		Other	
		DMVPN	Easy VPN	Remote Access	Site-to-Site	Firewall	Multicontext	Load Balancing	SSL
Catalyst 6500 Series Switches	Content-switching Services Modules	NA	NA	NA	NA	NA	NA	✓	NA
	Firewall Services Modules	NA	✓	✓	✓	✓	✓	NA	NA
	SSL Services Modules	NA	NA	NA	NA	NA	NA	NA	✓
	VPNSMs	✓	NA	—	✓	—	NA	NA	NA
	VPN SPAs	✓	NA	—	✓	—	NA	NA	NA
Cisco IOS VPN Routers		✓	✓	NA	✓	✓	NA	NA	NA
Cisco Integrated Services Routers		✓	✓	NA	✓	✓	NA	NA	NA
Cisco 7300 Series Routers		✓	✓	NA	✓	✓	NA	—	NA
PIX Security Appliances (known commonly as PIX Firewalls)		NA	✓	✓	✓	✓	✓	NA	NA
VPN 3000 Concentrator Series		NA	✓	✓	✓	NA	NA	NA	NA

- Cisco no longer sells VPNSM for Catalyst 6500 Series switches. We encourage you to migrate to VPN SPA, which supports DES and 3DES, as well as 128-, 192-, and 256-bit AES keys. See: <http://www.cisco.com/en/US/products/ps6917/index.html>.
- Supported services that vary for specific software or device versions:
 - PIX OS 7.0 and later support Easy VPN services, but not RAS clustering for Easy VPNs.
 - PIX OS 7.0 and later support Easy VPN, RAS VPN, site-to-site VPN, and virtual (multicontext) firewall services.
 - PIX OS 7.0 and later support RAS VPN and site-to-site VPN services in routed single context mode only.
 - FWSM versions 2.2 and later support virtual (multicontext) firewall services.
 - FWSM versions 3.1 and later support RAS VPN and site-to-site VPN services in routed single context mode only.
 - Cisco ASA Software Version 7.0 and later support Easy VPN, RAS VPN, site-to-site VPN, and virtual (multicontext) firewall services.
- Performance Monitor neither monitors nor offers reports for the load balancing of Cisco VPN 3000 concentrators or supported ASA appliances that you organize in virtual clusters. The *Load Balancing* column in this table refers exclusively to the web server load balancing services associated with supported content switching services modules in Catalyst 6500 series switches.

4. In this table:
- *NA* describes a service that the specified platform does not provide.
 - The em-dash character (—) describes a service that Performance Monitor does not monitor on the specified platform.

Related Topics

- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Working with Event Thresholds, page 21-28](#)
- [Configuring Performance Monitor as a Status Provider, page 21-17](#)

Supported Event Types for Each Service Type

To configure the threshold for device reachability, VPN tunnel status, or CPU usage event types, depending on the platform type, you need to enable the event type supported by a particular service. Configuring an event type under one of the services enables the threshold for that event type under all applicable services. [Table 21-5](#) describes only the events that affect the relevant service.

Table 21-5 *Event Types Supported for Service Types*

Monitored Service	Supported Event Types
Firewall	CPU Usage Device Accessible via Https Device Accessible via Snmp
Remote Access VPN	CPU Usage Device Accessible via Snmp
SSL	CPU Usage Device Accessible via Https
Site-to-Site VPN	CPU Usage Device Accessible via Https Device Accessible via Snmp Tunnel Status

Related Topics

- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Working with Event Thresholds, page 21-28](#)
- [Configuring Performance Monitor as a Status Provider, page 21-17](#)

Working with Event Thresholds

While Tunnel Status is a failure metric, CPU Usage and Device Accessible via Https or Device Accessible via Snmp are performance metrics. When you create a threshold, you:

- Define the boundaries of operational states (such as OK, Degraded, and Overloaded) for a performance metric or failure metric in a specific service.
- Specify the number of consecutive polling cycles during which an operational state must recur before records are updated.
- Associate a priority level with each possible operational state for a specific metric (for GUI display and user notification purposes).

Although the thresholds that you define use different services, metrics, and states, every threshold definition follows the same basic workflow.

**Tip**

When conditions exceed or fall below the thresholds that you define, Performance Monitor records an alarm that you can display and interpret in the relevant Event Browser.

This procedure describes how to configure thresholds for the event types.

Procedure

-
- Step 1** Select **Admin > Events**.
 - Step 2** Select a service from the TOC.
 - Step 3** Scan the entries in the Events list until you locate the performance metric or failure metric for which you plan to configure thresholds, then select the radio button in the relevant row.

Step 4 Click **Threshold**.

Tip You can also configure thresholds for an event if you select **Admin > Notifications**, then select an event and click **Threshold**.

A Threshold Configuration page appears. [Table 21-6](#) describes the elements in this page.

- If you select a failure metric, two opposite State Name values (such as Up and Down) appear in the Threshold Configuration page. Or, one extreme state value (such as OK) precedes multiple intermediate state values.
- If you select a performance metric, a range of State Name values (such as OK, Medium, and High) appears in the Threshold Configuration page; each value is associated with an upper and lower percentage in a range.

Step 5 Select the **Enable** check box.

You must select the Enable check box, or you cannot define values in a Threshold Configuration page.

Step 6 Do one of the following:

- If you see two opposite values (such as the benign *Up* and the problematic *Down*) in the State Name area, specify:
 - The event priority level for the problematic state.
 - The number of polling cycle failures that trigger, and the number of successes that clear, the event associated with the problematic state.
- If you see a range of three values in the State Name area, specify the upper and lower threshold percentages, polling cycle repetitions, and priority levels for each of the three values in the range.



Note When you configure thresholds for a performance metric, the lower threshold percentage for a benign state is always zero (0%), and the priority is always *OK*. The upper threshold percentage for a problematic state is always 100%. You cannot change these values.

Step 7 Do one of the following:

- To discard your selections and return to the Events page, click **Cancel**.

- To save and implement your selections, click **Apply**.
- To reset all values to their default settings and remain in the Threshold Configuration page, click **Default**.

Table 21-6 Threshold Configuration Page Elements

Element	Description
Common GUI Elements for All Thresholds	
Enable check box	Enables you to enable or disable the modification and implementation of threshold values.
State Name column	Displays two opposite states for a failure metric and a range of states for a performance metric.
Repetitions Before State Change column	Enables you to specify the number of consecutive polling cycles during which the relevant state must recur before Performance Monitor registers that the state has changed.
Event Priority column	Enables you to associate the relevant state with a priority level between P1 (the most severe) and P5 (the least severe).
Cancel button	Enables you to discard your changes and return to the Events page.
Apply button	Enables you to save and implement your threshold definitions for the current metric.
Default button	Enables you to reset all values to their default settings and remain in the Threshold Configuration page.
GUI Elements for Performance Thresholds Only	
Lower Threshold column	Enables you to select the percentage that defines the lower boundary of a state. For example, you could select 10% as the lower threshold boundary for the intermediate state. (Your selection would, in such a case, be applied automatically as the upper threshold percentage for the benign state.)

Table 21-6 Threshold Configuration Page Elements (continued)

Element	Description
Upper Threshold column	Displays a value that is equal to your definition of the lower threshold for the adjacent state, or displays 100% as the upper threshold for the problematic state.

Related Topics

- [Supported Services and Platforms for Monitoring and Reports, page 21-25](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Understanding the Events to be Monitored, page 21-18](#)
- [Supported Event Types for Each Service Type, page 21-27](#)
- [Configuring Performance Monitor as a Status Provider, page 21-17](#)

IPS Event Viewer

The Cisco IPS Event Viewer (IEV) offers a free monitoring solution for small-scale IPS deployments. Monitoring individual IPS devices, IEV is easy to set up and use, and provides the following capabilities:

- Support for IPv6 through SDEE compatibility
- Customized reporting
- Configurable notification actions such as email and paging
- Visibility into applied response actions, virtual sensor ID, learned DST OS, and threat rating

IEV is a Java-based application that lets you view and manage alerts for up to five sensors. With IEV, you can connect to and view alerts in real time or in imported log files. You can configure filters and views to help you manage the alerts and import and export event data for further analysis. IEV reports the top alerts, attackers, and victims over a specified number of hours or days. IEV also provides access to MySDN for signature descriptions. See Cisco IPS Event Viewer Version 5.2 documentation for more information.

You can start IEV from Security Manager as a client-server application. IEV server is installed when you install the Security Manager server. When you start IEV on a Security Manager client, the IEV client files are obtained from the Security Manager server and copied to the folder where the Security Manager client was installed on your client system. The IEV client files are uninstalled when you uninstall the Security Manager client on your client system. The requirements and dependencies for installing IEV server and client are the same as those for Security Manager server and client software.

**Note**

To enable communication between IEV server and IEV client, you need to modify the Cisco Security Agent or any other anti-virus and network firewall software policies on the Security Manager server to configure TCP ports 60002 and 60003 as open ports. If the server has a preexisting installation of the full Cisco Security Agent, the standalone agent is not installed on the system when you install Security Manager. In such a case, configure the Cisco Security Agent network services to accept connections on TCP ports 60002 and 60003. However, if the server on which you install Security Manager was not previously installed with the full, commercial version of Cisco Security Agent, the Security Manager installer installs a customized, standalone agent on your server and opens the necessary TCP ports for communication between IEV server and IEV client.

When you start IEV client from the Security Manager client system, IEV client automatically opens TCP port 5001 to establish communication with the IEV server.

**Note**

Although IEV is displayed in the list of installed programs in the Add/Remove Programs window after installation, we recommend that you uninstall IEV using the Security Manager uninstaller instead of using the Add/Remove Programs control panel.

**Note**

When you install Security Manager in a high availability (HA) or data redundancy (DR) deployment configuration, the Security Manager installer application does not install IEV server on your server system. The functionality to start IEV client from your Security Manager client is available only when Security Manager is configured in a non-HA/DR environment.

**Caution**

Disable any anti-virus or host-based intrusion detection software before beginning the Security Manager server installation. Close any open applications. The Wise installer, which is a commercially available Windows Installer (MSI) package, spawns a command shell application that can trigger your host-based detection software, which causes the IEV installation to fail.

To verify IEV server installation, follow these steps:

Step 1

Review the `<path to Cisco IPS Event Viewer>/IEV/log/system.log` file. It should only contain the following message:

```
Cisco IPS Event Viewer service successfully started.
```

Step 2

Select **Start > Settings > Control Panel > Administrative Tools > Services** to verify that the following Windows services have started:

- Cisco IPS Event Viewer service

This service lets IEV retrieve alerts from remote device(s), store alerts in the MySQL database, archive database files, and check for available disk space.

- MySQL service

This service controls the persistent storing and serving of data.

**Note**

The Cisco IPS Event Viewer service depends on MySQL services. If you want to stop retrieving alerts, you can stop the Cisco IPS Event Viewer service. Later you can restart the Cisco IPS Event Viewer service to resume retrieving and storing alerts.

**Caution**

Do not remove the `c:\my.cnf` file. The MySQL server used by IEV requires this file.

IEV server is uninstalled when you uninstall Security Manager server.

Related Topics

- [Understanding Communication, page 21-34](#)
- [Guidelines for Working with IEV from Security Manager, page 21-35](#)
- [Starting IEV Client, page 21-37](#)

Understanding Communication

Security Manager client intercepts all SSL requests made by IEV client and sends them to the IEV server running on Security Manager server. IEV server processes the requests redirected by the IEV client by obtaining information from the sensor or sending data such as the IEV image to the client. This communication between the IEV client and IEV server is transparent to the IPS sensor, and appears as though there is a direct connection between IEV client and the sensor.

The Cisco IPS Event Viewer and MySQL services must be running on the IEV server to enable IEV monitor sensors. IEV server retrieves the events from IPS sensors and stores them in the MySQL database. When you start the IEV client from Security Manager client, a secure connection is established between IEV client and IEV server, the Java application on the IEV client reads the event details from the MySQL database, and event data is displayed on the IEV client in various views, tables, and graphs.

If the IEV client files are not available in the client cache directory, the image is obtained from the Security Manager server. The Security Manager client starts only one instance of IEV client and closes the IEV client window when you exit the Security Manager client or when the idle session timeout period is exceeded.

Related Topics

- [IPS Event Viewer, page 21-31](#)
- [Guidelines for Working with IEV from Security Manager, page 21-35](#)
- [Starting IEV Client, page 21-37](#)
- [Navigating to IPS Signature Policy in Security Manager from IEV, page 21-37](#)

Guidelines for Working with IEV from Security Manager

Keep in mind the following guidelines when working with IEV started from Security Manager:

- IEV enables you to view alarms for up to five sensors at a time.
- IEV uses the same JRE version as Security Manager.
- IEV client is not preinstalled with Ethereal or any packet sniffer.
- If Ethereal was previously installed on your computer when you install Security Manager, you need to specify the directory where Ethereal was installed from the IEV main menu. You also need to modify the location of Ethereal if you later move the Ethereal executable file to a different directory or if you decide to install Ethereal after installing Security Manager.



Note

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 and view 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.

- Cisco IPS Event Viewer and MySQL services are installed as Windows NT services.
- All IEV client-side runtime files, such as client log files and cache files, are copied to the subdirectory under the Security Manager client installation directory. The default location for these files is C:\Program Files\Cisco Systems\Cisco Security Manager Client\cache.
- All IEV server-side files, databases, log files, configuration files and other runtime files are installed in a subdirectory under the Security Manager server installation directory. The default location for these files is C:\Program Files\CSCOPx\IPSEventViewer.
- If you attempt to install IEV server on a Security Manager server system that has been already installed with IEV from Cisco.com, an error message is displayed.

- You can start only one instance of IEV client per Security Manager client system.
- You can start multiple IEV clients for the same IEV server at the same time from different Security Manager clients systems.
- You cannot start IEV client from a Security Manager client if the Security Manager server has also been installed on the same system.
- If you installed IEV server on a system using the Security Manager installer, you cannot install IEV separately from Cisco.com on the same system.
- If you installed IEV server on a system using the Security Manager installer, IEV server is not reinstalled when you attempt to reinstall Security Manager on the same system.
- Before IEV can receive events from a sensor, you must add the sensor to the list of devices that IEV monitors and specify the device credentials. See Cisco IPS Event Viewer Version 5.2 documentation for information on how to add a sensor to be monitored by IEV. You must also add the sensor to the Security Manager inventory to view event data from the sensors you are monitoring.
- When you want to stop receiving events from a sensor, you must remove the sensor from the list of devices that IEV monitors and from the Security Manager inventory separately. IEV terminates the connection to that sensor and no longer receives events from that sensor.
- Backup and restore of the Security Manager database does not apply to IEV database.
- IEV log files are archived when you generate the Security Manager diagnostics file.
- When you exit the Security Manager client, the IEV client window is closed.

Related Topics

- [IPS Event Viewer, page 21-31](#)
- [Understanding Communication, page 21-34](#)
- [Starting IEV Client, page 21-37](#)

Starting IEV Client

This procedure describes how to start an IEV client from the Security Manager client.

Before You Begin

- Make sure the Windows NT services for IEV server are running on the Security Manager server. To review the status of the Cisco IEV and MySQL services, select **Start > Settings > Control Panel > Administrative Tools > Services**.
- Make sure you selected an IPS sensor from the Device selector.

Procedure

Step 1 Select **Tools > IPS Event Viewer**.

A dialog box asks you to confirm that you want to start IEV client from the Security Manager client.

Step 2 Click **Yes** to continue.

The IEV client window is displayed when the start operation is complete.

Related Topics

- [IPS Event Viewer, page 21-31](#)
- [Understanding Communication, page 21-34](#)
- [Guidelines for Working with IEV from Security Manager, page 21-35](#)
- [Navigating to IPS Signature Policy in Security Manager from IEV, page 21-37](#)

Navigating to IPS Signature Policy in Security Manager from IEV

Sensors use signatures to determine whether the contents of network packets meet the criteria of an attack. A signature is 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 enables

you to configure signatures for Cisco IPS sensors. When the packets match a given signature rule, the sensor generates an alarm. You can configure IEV to manage alarms from sensors by adding the sensors to the IEV Devices folder.

After you add the device to IEV, IEV sends a subscription request to the sensor. IEV will receive alerts and events from the sensor, beginning with the first event the sensor receives after connecting with IEV. An event is an IPS message that contains an alert, a block request, a status message, or an error message.

Using IEV, you can select an event generated by an IPS signature from the log of events within the Realtime Dashboard or the View folders, and 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 to handle network attacks. The following sections describe how to look up the Signatures policy page in Security Manager from IEV:

- [IPS Signature Policy Lookup from the Realtime Dashboard, page 21-38](#)
- [IPS Signature Policy Lookup from the Views Tab, page 21-39](#)

IPS Signature Policy Lookup from the Realtime Dashboard

You can use the Realtime Dashboard to view a continuous stream of real-time events from the 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 the sensor(s) and the maximum number of events to display.

This procedure describes how to look up an IPS signature in the Signatures policy page of Security Manager from the Realtime Dashboard of IEV:

Step 1 Open IEV client from the Security Manager client. For a description of the procedure to start IEV client, see [Starting IEV Client, page 21-37](#).

Step 2 Choose **Tools > Realtime Dashboard > Launch Dashboard**.

IEV opens a subscription request with the sensor. If the connection is successful, the Realtime Dashboard appears and displays the most recent events received by the sensor since the request was opened.

Step 3 Right-click a row associated with an event, then select **Go to CSM**. The Security Manager client window is activated and the Signatures policy page appears with the IPS signature that generated the event highlighted in the policy table.

For each event entry in IEV, Security Manager searches all the signatures within the context of your current activity when Workflow mode is enabled (including policies defined in your private view and saved locally on the client, and policies committed to the Security Manager database), or current login session when non-Workflow mode is enabled. If the event entry had been triggered by a signature not referenced in the current activity, an error message appears.

You can edit the signature that triggered the event by right-clicking its row in the table and selecting **Edit Row** from the Row Context Menu.

Related Topics

- [IPS Signature Policy Lookup from the Views Tab, page 21-39](#)
- [Navigating to IPS Signature Policy in Security Manager from IEV, page 21-37](#)

IPS Signature Policy Lookup from the Views Tab

The Views tab lets you analyze filtered event data from a specified source. IEV ships with five default views; however, you can use the View Wizard to create and store user-defined views in the Views folder. Based on the data that is populated in a specific view, you can navigate to the events. For example, you can select the view configured to group events by signature name to organize the table of events by signature name. You can expand an event to view the details, such as signature name and severity level, associated with that event, and navigate to the Signatures policy in Security Manager.

IEV lets you access various tables and graphs that provide specialized views into the event data you are analyzing. Before you create a view and begin working with the individual tables and graphs, review the following descriptions.

The following tables organize the events for a view. The events shown in these tables and graph differ depending on the data source you choose for the view. The data source can be the event_realtime_table, archived tables, or imported log files.

- Alert Aggregation table—The first table displayed for any view. You access an alert aggregation table by double-clicking the view name in the Views folder.
- Expanded Details Dialog table—Displays the details of a particular event listed in an alert aggregation table. You access the Expanded Details Dialog table by right-clicking a row in the first column of an alert aggregation table.
- Drill Down Dialog table—Displays the individual entries for a particular column in the alert aggregation table, such as the individual source addresses associated with a UDP Bomb event. You access the Drill Down Dialog table by double-clicking a column (except first or Total Alarm Count) in an alert aggregation table.
- Alarm Information Dialog table—Displays the individual alerts for a particular event. You access the Alarm Information Dialog table by double-clicking the Total Alarm Count column in the alert aggregation table, or by right-clicking the first column of the Expanded Details Dialog table.

See Cisco IPS Event Viewer Version 5.2 documentation for more information.

This procedure describes how to look up an IPS signature in the Signatures policy page of Security Manager from the Views folder of IEV:

-
- Step 1** Open IEV client from the Security Manager client. For a description of the procedure to start IEV client, see [Starting IEV Client, page 21-37](#).
- Step 2** Click the **Views** tab.
- Step 3** Double-click the **Views** folder to view the list of defined views.
- Step 4** To view individual alarms associated with an event from an alert aggregation table, do the following:
- a. Right-click a cell in the first column in an alert aggregation table associated with the event you want to expand, and then choose **Expand Whole Details**.
The Expanded Details Dialog appears with the Whole Address tab displayed.
 - b. To view the events by address category, click the **Class A Level**, **Class B Level**, or **Class C Level** tab.
 - c. Right-click any column in the Expanded Details Dialog, then select **View Alarms**.
The Alarm Information Dialog appears.

**Tip**

You also access the Alarm Information Dialog by double-clicking a column (except first or Total Alarm Count) in an alert aggregation table, right-clicking a cell in the first column from the Drill Down Dialog, and selecting **View Alarms**.

**Note**

For cells that display an arrow (—>) after the number of occurrences, double-click that cell to display the contents of the cell.

A second table appears in the Drill Down Dialog and displays the contents of the cell. Double-clicking a cell containing an arrow (—>) in this second table displays the Alarm Information Dialog.

- Step 5** Right-click a row associated with an event, then select **Go to CSM**. The Security Manager client window is activated and the Signatures policy page appears with the IPS signature that generated the event highlighted in the policy table.

For each event entry in IEV, Security Manager searches all the signatures within the context of your current activity when Workflow mode is enabled (including policies defined in your private view and saved locally on the client, and policies committed to the Security Manager database), or current login session when non-Workflow mode is enabled. If the event entry had been triggered by a signature not referenced in the current activity, an error message appears.

You can edit the signature that triggered the event by right-clicking its row in the table and selecting **Edit Row** from the Row Context Menu.

Related Topics

- [IPS Signature Policy Lookup from the Realtime Dashboard, page 21-38](#)
- [Navigating to IPS Signature Policy in Security Manager from IEV, page 21-37](#)

Security Manager Access Rule Lookup from Device Manager Syslog

Each interface on the device or appliance is associated with a list of ACEs that are associated with an ACL. When the firewall device finds a matching ACE, the device performs the associated action either permitting the packet into the firewall device for further processing, or denying entry to the packet. If no ACE matches the packet, the packet is denied. Activity on your firewall or router is monitored through the creation of syslog entries. If logging is enabled on the device, whenever an access rule that is configured to generate syslog entries is invoked—for example, if a connection were attempted from a denied IP address—a log entry is generated.

Security Manager 3.1 introduces a new Syslog to Access Rule Correlation tool that enhances day-to-day security management and troubleshooting activities. With this tool, you can quickly resolve common configuration issues, along with most user and network connectivity problems. Because the configuration process is simple, operational efficiency and response times for business-critical functions are improved. For ASDM and SDM started from within Security Manager, you can identify the ACL on a router or firewall that generated a syslog message received by ASDM and SDM. The access rule that triggered the syslog entry is highlighted on a first-match basis, even if there are multiple access rules that cause the same syslog message to be generated. The feature to perform the Security Manager policy table lookup, when the device generates a syslog message, is available in SDM 2.3.4, which supports all versions of Cisco IOS software running on a router, ASDM 5.2(2), which manages ASA 7.2, and ASDM 5.0(1)F, which runs with FWSM 3.1.

Using ASDM 5.2.2 and 5.0(1)F, you can select a syslog message generated by an ACL within the Real-time Log Viewer window or Log Buffer Viewer window, and navigate to the access control rule in Security Manager for that specific syslog. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules. You can closely observe enterprise traffic patterns and monitor resource access behavior. For more information, see [Navigating to ACL in Security Manager from ASDM Syslog, page 21-43](#).

Using SDM 2.3.4, you can select a syslog message generated by an ACL from the log of events categorized by security level and displayed under the Syslog tab of the Logging window. For each selected syslog message, you can look up the

Security Manager to highlight the access control entry that matches the traffic that generated the message. You can then disable the rule to permit or deny the traffic. For more information, see [Navigating to ACL in Security Manager from SDM Syslog](#), page 21-46.

Related Topics

- [Navigating to ACL in Security Manager from ASDM Syslog](#), page 21-43
- [Navigating to ACL in Security Manager from SDM Syslog](#), page 21-46

Navigating to ACL in Security Manager from ASDM Syslog

The Log viewing feature of ASDM lets you view real-time system log messages that appear in the log buffer. When you start ASDM from Security Manager, the most recent ASDM system log messages appear at the bottom of the ASDM home page. The Log Buffer panel enables you to view log messages saved in the buffer in a separate window. Depending on the level of logging messages to view, ranging from Emergency to Debugging, and click **View** to open a separate window in which log messages appear. The Log Buffer window displays the identification number of the log message, date and time that the system log messages was generated, the logging level of a syslog message, and the addresses of the network or host from which the packet is being sent and received. You can select a syslog message and identify the ACL in Security Manager that created the log message.

This procedure describes how to look up the access rule in the policy table of Security Manager from the Log Buffer panel of ASDM.

Procedure

-
- Step 1** Open ASDM from the Security Manager client. For a description of the procedure to start device manager, see [Starting Device Manager from Security Manager](#).
 - Step 2** Perform one of the following:
 - From ASDM 5.2(2), select **Monitoring > Logging > Log Buffer**. The Log Buffer panel appears.
 - From ASDM 5.0(1)F, select **Monitoring > Features > Logging > Log Buffer**. The Log Buffer panel appears.
 - Step 3** Click **View** to display the log messages currently in the buffer. The Log Buffer window opens as a separate window.

- Step 4** Right-click a syslog message generated by a firewall access rule, then select **Goto Rule in CSM**. The Security Manager client window is activated and the Access Rules page appears with the access rule that generated the syslog message highlighted in the policy table.



Note If you try to navigate to Security Manager from a syslog message that was not generated by a firewall access rule, a popup window prompts you to select a message generated by an ACL.

For each syslog entry, Security Manager searches all the access rules within the context of your current activity when Workflow mode is enabled (including policies defined in your private view and saved locally on the client, and policies committed to the Security Manager database), or current login session when non-Workflow mode is enabled. If the syslog entry had been triggered by an access rule not referenced in the current activity, an error message appears.

You can edit the access rule that triggered the syslog message in their entirety by double-clicking a rule number in the table, or edit individual table cells by double-clicking a cell.

If you did not close any modal dialog box in Security Manager, navigation to the access rule in the policy table fails from ASDM. Close the modal dialog box and try to invoke the access rule in Security Manager again.



Note Security Manager uses modal dialog windows to display warnings or user notification messages. Generally, when an application displays a modal window or dialog, the application stops responding to any event (mouse action, keyboard entry, and so on) other than the event associated with the modal window (you must first respond to the modal window). If you overlay the modal window with any other application window (the modal window now is “invisible”), the application appears frozen. If your browser window appears frozen, ensure that there is no modal window that has inadvertently been covered.

The Real-time Log Viewer panel enables you to view real-time system log messages in a separate window. Depending on the level and maximum number of logging messages to view, click **View** to display a separate window in which log

messages appear. The Real-time Log Viewer window enables you to view incoming messages in real time and look up the ACL that generated the syslog message.

This procedure describes how to look up the access rule in the policy table of Security Manager from the Real-time Log Viewer panel of ASDM.

Procedure

- Step 1** Open ASDM from the Security Manager client. For a description of the procedure to start device manager, see [Starting Device Manager from Security Manager](#).
- Step 2** Perform one of the following:
- From ASDM 5.2(2), select **Monitoring > Logging > Real-time Log Viewer**. The Real-time Log Viewer panel appears.
 - From ASDM 5.0(1)F, select **Monitoring > Features > Logging > Live Log**. The Live Log Viewer panel appears.
- Step 3** Click **View** to display the incoming log messages on the security appliance in real-time. The Real-time Log Viewer window opens as a separate instance.
- Step 4** Right-click a syslog message generated by an ACL, then select **Goto Rule in CSM**. The Security Manager client window is activated and the Access Rules page appears with the access rule that generated the syslog message highlighted in the policy table.



Note If you try to navigate to Security Manager from a syslog message that was not generated by a firewall access rule, a popup window prompts you to select a message generated by an ACL.

For each syslog entry, Security Manager searches all the access rules within the context of your current activity when Workflow mode is enabled (including policies defined in your private view and saved locally on the client, and policies committed to the Security Manager database), or current login session when non-Workflow mode is enabled. If the syslog entry had been triggered by an access rule not referenced in the current activity, an error message appears.

You can edit the access rule that triggered the syslog message in their entirety by double-clicking a rule number in the table, or edit individual table cells by double-clicking a cell.

Related Topics

- [Navigating to ACL in Security Manager from SDM Syslog, page 21-46](#)

Navigating to ACL in Security Manager from SDM Syslog

SDM 2.3.4 offers the following logs:

- **Syslog**—The router contains a log of events categorized by severity level. It is the router log that is displayed, even if log messages are being forwarded to a syslog server.
- **Firewall Log**— The log entries shown in the top part of this window are determined by log messages generated by the firewall. In order for the firewall to generate log entries, you must configure individual access rules to generate log messages when they are invoked.
- **Application Security Log**—If logging has been enabled, and you have specified that alarms be generated when the router encounters traffic from applications or protocols that you have specified, those alarms are collected in a log that can be viewed from this window.
- **SDEE Message Log**—If SDEE has been configured on the router, this log records SDEE messages. SDEE messages are generated when there are changes to IPS configuration.

This procedure describes how to look up the access rule in the policy table of Security Manager from the Logging panel of SDM 2.3.4.

Procedure

- Step 1** Open SDM from the Security Manager client. For a description of the procedure to start device manager, see [Starting Device Manager from Security Manager](#).
- Step 2** Select **Monitor > Logging**. The Logging panel appears with Syslog tab displayed. You can also open it by clicking the Syslog tab from any other tab in the Logging panel.

- Step 3** Select a syslog message generated by an access rule, then click the **Goto Rule in CSM** button above the table of log messages displayed. The Security Manager client window is activated and the Access Rules page appears with the access rule that generated the syslog message highlighted in the policy table.



Note If you try to navigate to Security Manager from a syslog message that was not generated by a firewall access rule, a popup window prompts you to select a message generated by an ACL.

For each syslog entry, Security Manager searches all the access rules within the context of your current activity when Workflow mode is enabled (including policies defined in your private view and saved locally on the client, and policies committed to the Security Manager database), or current login session when non-Workflow mode is enabled. If the syslog entry had been triggered by an access rule not referenced in the current activity, an error message appears.

You can edit the access rule that triggered the syslog message in their entirety by double-clicking a rule number in the table, or edit individual table cells by double-clicking a cell.

Related Topics

- [Security Manager Access Rule Lookup from Device Manager Syslog, page 21-42](#)
- [Navigating to ACL in Security Manager from SDM Syslog, page 21-46](#)

