Getting Started with IPS Configuration

Cisco Intrusion Prevention System (IPS) Sensors are network devices that perform real-time monitoring of network traffic for suspicious activities and active network attacks. The IPS sensor analyzes network packets and flows to determine whether their contents appear to indicate an attack against your network.

Using Cisco Security Manager, you can configure and manage sensors, which can be dedicated stand-alone network appliances, Catalyst 6500 switch modules, service modules running in supported ASA devices or routers, and IPS-enabled Cisco IOS Software images running on integrated services routers. For a full list of supported IPS devices and software versions, see the Supported Devices and Software Versions for Cisco Security Manager document for this version of the product.

This chapter contains the following topics:

- Understanding IPS Network Sensing , on page 1
- Overview of IPS Configuration , on page 5
- Identifying Allowed Hosts , on page 8
- Configuring SNMP , on page 9
- Managing User Accounts and Password Requirements , on page 16
- Identifying an NTP Server , on page 24
- Identifying DNS Servers , on page 25
- Identifying an HTTP Proxy Server , on page 26
- IPS SSHv2 Known Host Keys, on page 27
- Configuring IPS SSHv1 Fallback Settings, on page 28
- Configuring the External Product Interface , on page 28
- Configuring IPS Logging Policies , on page 32
- IPS Health Monitor, on page 33
- Configuring IPS Security Settings, on page 35

Understanding IPS Network Sensing

Network sensing can be accomplished using Cisco IPS sensors (appliances, switch modules, network modules, and SSMs) and Cisco IOS IPS devices (Cisco IOS routers with IPS-enabled images and Cisco ISRs). These sensing platforms are components of the Cisco Intrusion Prevention System and can be managed and configured through Cisco Security Manager. These sensing platforms monitor and analyze network traffic in real time. They do this by looking for anomalies and misuse on the basis of network flow validation, an extensive embedded signature library, and anomaly detection engines. However, these platforms differ in how they can respond to perceived intrusions.

Tip Cisco IPS sensors and Cisco IOS IPS devices are often referred to collectively as IPS devices or simply sensors. However, Cisco IOS IPS does not run the full dedicated IPS software, and its configuration does not include IPS device-specific policies. Additionally, the amount of sensing that you can perform with Cisco IOS IPS is more limited. The following sections focus on using dedicated IPS devices, including service modules installed in IOS routers, rather than Cisco IOS IPS. For a discussion focused on Cisco IOS IPS, see Intrusion Prevention System (IPS) Cisco IOS Intrusion Prevention System Deployment Guide on Cisco.com and Configuring IOS IPS Routershttp://www.cisco.com/go/iosips .

When an IPS device detects unauthorized network activity, it can terminate the connection, permanently block the associated host, and take other actions.

Note For more overview information on IPS sensors, including a comparison of the available appliances and service modules and details about device interfaces, see Introducing the Sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules* . A list of these documents for each IPS release is available at http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_installation_guides_list.html .

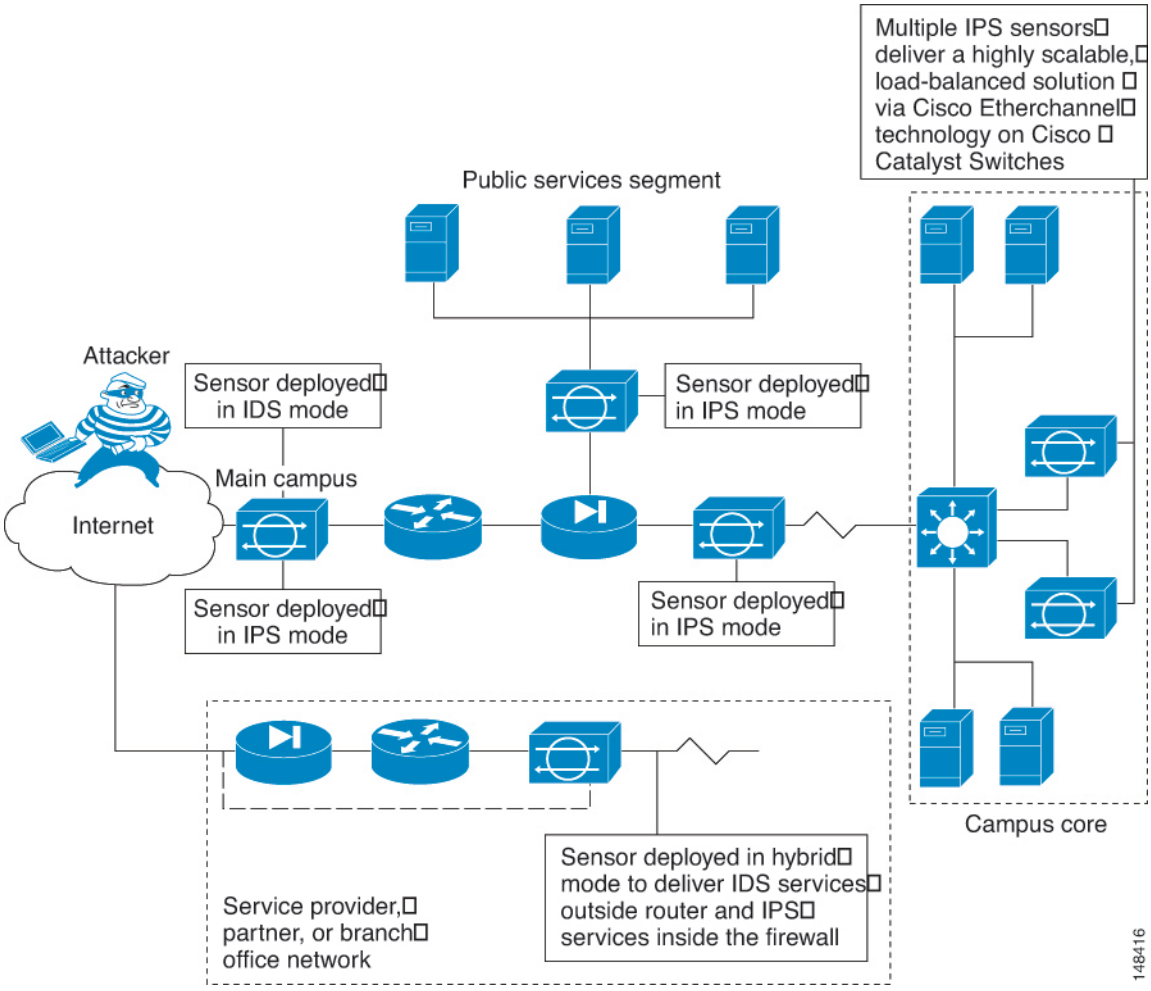
This section contains the following topics:

- Capturing Network Traffic , on page 2
- Correctly Deploying the Sensor , on page 4
- Tuning the IPS , on page 4

Capturing Network Traffic

The sensor can operate in either promiscuous or inline mode. The following illustration shows how you can deploy a combination of sensors operating in both inline (IPS) and promiscuous (IDS) modes to protect your network.

Figure 1: Comprehensive IPS Deployment Solutions



The command and control interface is always Ethernet. This interface has an assigned IP address, which allows it to communicate with the manager workstation or network devices (Cisco switches, routers, and firewalls). Because this interface is visible on the network, you should use encryption to maintain data privacy. SSH is used to protect the CLI and TLS/SSL is used to protect the manager workstation. SSH and TLS/SSL are enabled by default on the manager workstations.

When responding to attacks, the sensor can do the following:

- Insert TCP resets via the sensing interface.

Note You should select the TCP reset action only on signatures associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol.

- Make ACL changes on switches, routers, and firewalls that the sensor manages.

Note ACLs may block only future traffic, not current traffic.

- Generate IP session logs, session replay, and trigger packets display.

IP session logs are used to gather information about unauthorized use. IP log files are written when events occur that you have configured the appliance to look for.

- Implement multiple packet drop actions to stop worms and viruses.

Correctly Deploying the Sensor

Before you deploy and configure your sensors, you should understand the following about your network:

- The size and complexity of your network.
- Connections between your network and other networks, including the Internet.
- The amount and type of traffic on your network.

This knowledge will help you determine how many sensors are required, the hardware configuration for each sensor (for example, the size and type of network interface cards), and how many managers are needed.

You should always position the IPS sensor behind a perimeter-filtering device, such as a firewall or adaptive security appliance. The perimeter device filters traffic to match your security policy thus allowing acceptable traffic in to your network. Correct placement significantly reduces the number of alerts, which increases the amount of actionable data you can use to investigate security violations. If you position the IPS sensor on the edge of your network in front of a firewall, your sensor will produce alerts on every single scan and attempted attack even if they have no significance to your network implementation. You will receive hundreds, thousands, or even millions of alerts (in a large enterprise environment) that are not really critical or actionable in your environment. Analyzing this type of data is time consuming and costly.

Tuning the IPS

Tuning the IPS ensures that the alerts you see reflect true actionable information. Without tuning the IPS, it is difficult to do security research or forensics on your network because you will have thousands of benign events, also known as false positives. False positives are a by-product of all IPS devices, but they occur much less frequently in Cisco IPS devices because Cisco IPS devices are stateful, normalized, and use vulnerability signatures for attack evaluation. Cisco IPS devices also provide risk rating, which identifies high risk events, and policy-based management, which lets you deploy rules to enforce IPS signature actions based on risk rating.

Follow these tips when tuning your IPS sensors:

- Place your sensor on your network behind a perimeter-filtering device.

Proper sensor placement can reduce the number of alerts you need to examine by several thousands a day.

- Deploy the sensor with the default signatures in place.

The default signature set provides you with a very high security protection posture. The Cisco signature team has spent many hours on testing the defaults to give your sensor the highest protection. If you think that you have lost these defaults, you can restore them.

- Make sure that the event action override is set to drop packets with a risk rating greater than 90.

This is the default and ensures that high risk alerts are stopped immediately.

- Filter out known false positives caused by specialized software, such as vulnerability scanner and load balancers by one of the following methods:
  - You can configure the sensor to ignore the alerts from the IP addresses of the scanner and load balancer.
  - You can configure the sensor to allow these alerts and then use Event Viewer to filter out the false positives.
- Filter the Informational alerts.

These low priority events notifications could indicate that another device is doing reconnaissance on a device protected by the IPS. Research the source IP addresses from these Informational alerts to determine what the source is.

- Analyze the remaining actionable alerts:
  - Research the alert.
  - Fix the attack source.
  - Fix the destination host.
  - Modify the IPS policy to provide more information.

Overview of IPS Configuration

There are a wide variety of devices on which you can configure the Intrusion Prevention System. From a configuration point-of-view, you can separate the devices into two groups: dedicated appliances and service modules (for routers, switches, and ASA devices) that run the full IPS software; and IPS-enabled routers running Cisco IOS Software 12.4(11)T and later (Cisco IOS IPS).

The following procedure is an overview of IPS configuration on dedicated appliances and service modules. For Cisco IOS IPS devices (which does not include IPS service modules installed in a router), see Overview of Cisco IOS IPS Configuration.

Procedure

Step 1 Install and connect the device to your network. Install the device software and perform basic device configuration. Install the licenses required for all of the services running on the device. The amount of initial configuration that you perform influences what you will need to configure in Security Manager.

Follow the instructions in the Installing Cisco Intrusion Prevention System Appliances and Modules document for the IPS version you are using.

Step 2 Add the device to the Security Manager device inventory (see Adding Devices to the Device Inventory).

Tip
You can discover router and Catalyst switch modules when adding the device in which the module is installed. For ASA devices, you must add the service module separately.

Step 3 Configure the interfaces as described in Configuring Interfaces. You must enable the interfaces connected to your network for the device to function.

For certain types of service module, there are additional policies to configure:

- Router-hosted service modules—Configure the **IPS Module** interface settings policy on the router. For more information, see IPS Module Interface Settings on Cisco IOS Routers.
- IDSM—Configure the **IDSM Settings** Catalyst platform policy. For more information, see IDSM Settings.
- IPS modules on ASA devices—Configure the **Platform > Service Policy Rules > IPS, QoS, and Connection Rules** policy on the host ASA to specify the traffic that should be inspected. For more information, see About IPS Modules on ASA Devices and Service Policy Rules Page.

Step 4 Use the **Virtual Sensors** policy to assign interfaces to the virtual sensors, including the base vs0 virtual sensor that exists for all IPS devices. For information about virtual sensor settings and assigning interfaces to a virtual sensor, see Defining A Virtual Sensor.

If the device supports it, and you have a need for it, you can also create user-defined virtual sensors so that a single device acts like multiple sensors. Most of the IPS configuration is done on the parent device, but you can configure unique settings per virtual sensor for signatures, anomaly detection, and event actions. For more information, see Configuring Virtual Sensors.

Step 5 Configure basic device access platform policies. These policies determine who can log into the device:

- **AAA**—Configure this policy if you want to use a RADIUS server to control access to the device. You can use AAA control in conjunction with local user accounts defined in the User Accounts policy. See Configuring AAA Access Control for IPS Devices , on page 22.
- **Allowed Hosts**—The addresses of hosts who are allowed access. Ensure that the Security Manager server is included as an allowed host, or you cannot configure the device using Security Manager. See Identifying Allowed Hosts , on page 8.
- **SNMP**—Configure this policy if you want to use an SNMP application to manage the device. See Configuring SNMP , on page 9.
- **Password Requirements**—You can define the acceptable characteristics of a user password. See Configuring User Password Requirements , on page 21.
- **User Accounts**—The user accounts defined on the device. See Configuring IPS User Accounts , on page 19.

Step 6 Configure basic server access platform policies. These policies identify the servers to which the device can connect:

- **External Product Interface**—If you use Management Center for Cisco Security Agents, configure this policy to allow the sensor to download host postures from the application. See Configuring the External Product Interface , on page 28.
- **NTP**—Configure this policy if you want to use a Network Time Protocol server to control the device time. See Identifying an NTP Server , on page 24.

- **DNS, HTTP Proxy**—The DNS and HTTP Proxy policies are required only if you configure global correlation. They identify a server that can resolve DNS names to IP addresses. Use the HTTP Proxy policy if your network requires the use of a proxy to make Internet connections; otherwise, use the DNS policy. See Identifying DNS Servers , on page 25 or Identifying an HTTP Proxy Server , on page 26.

Step 7 Configure the Logging policy if you want non-default logging. See Configuring IPS Logging Policies , on page 32.

Step 8 Configure IPS signatures and event actions. Event action policies are easier to configure than creating custom signatures, so try to use event action filters and overrides to modify signature behavior before trying to edit specific signatures. For more information, see the following topics:

- Configuring Event Action Rules
- Configuring Signatures

Step 9 If you use any of the Request Block or Request Rate Limit event actions, configure blocking or rate limiting hosts. See Configuring IPS Blocking and Rate Limiting.

Step 10 Configure other desired advanced IPS services. See the following topics:

- Configuring Global Correlation
- Configuring Anomaly Detection

Step 11 Maintain the device:

- Update and redeploy configurations as necessary.
- Apply updated signature and engine packages. For information about checking for updates, applying them, and setting up regular automated updates, see Managing IPS Updates.
- Manage the device licenses. You can update and redeploy licenses, or automate license updates. For more information, see the following topics:
  - Updating IPS License Files
  - Redeploying IPS License Files
  - Automating IPS License File Updates
- Manage the certificates required for SSL (HTTPS) communication. These certificates expire, so you need to regenerate them approximately every 2 years. For information on regenerating certificates and ensuring that the certificates defined on the device are synchronized with those stored in the Security Manager certificate store, see Managing IPS Certificates.

Step 12 Monitor the device:

- Use the Event Viewer application to view alerts generated from the device. You can open Event Viewer from the Launch menu in Configuration Manager or Report Manager, or from the Windows Start menu.
  - For information on using Event Viewer, see Viewing Events.
  - For an example of how to filter IPS alerts, see Removing False Positive IPS Events from the Event Table.
- Use the Report Manager application to generate reports on IPS usage, including comparisons of inline vs. promiscuous mode, and global correlation vs. traditional inspection. You can also analyze top attackers, victims,

signatures, blocked signatures, and perform target analysis. The following topics explain Report Manager and the IPS reports in more detail:

- Managing Reports
- Understanding General IPS Reports
- Understanding IPS Top Reports
- Opening and Generating Reports

Identifying Allowed Hosts

Use the Allowed Hosts policy to identify which hosts or networks have permission to access the IPS sensor. By default, no hosts are permitted to access a sensor, so you must add hosts or networks to this policy.

Specifically, you must add either the IP address of the Security Manager server, or its network address, or Security Manager cannot configure the device. Also add the addresses of all other management hosts that you use, such as CS-MARS.

Tip If you add host addresses only, you will be limited to using those workstations to access the device. Instead, you can specify network addresses to allow all hosts connected to specific "safe" networks access.

Procedure

Step 1 Do one of the following to open the Allowed Hosts policy:

- (Device view) Select **Platform** > **Device Admin** > **Device Access** > **Allowed Hosts** from the Policy selector.
- (Policy view) Select **IPS** > **Platform** > **Device Admin** > **Allowed Hosts**, then select an existing policy or create a new one.

Step 2 Do one of the following:

- To add an entry, click the **Add Row** button and fill in the Access List dialog box.

You can add up to 512 entries.

- To edit an entry, select it and click the **Edit Row** button.
- To delete an entry, select it and click the **Delete Row** button.

Step 3 When adding or editing an entry, specify the host or network address in the Add or Modify Access List dialog box, then click **OK**. You can enter addresses using the following formats:

- Host address—A simple IP address, such as 10.100.10.10.
- Network address—A network address and mask, such as 10.100.10.0/24 or 10.100.10.0/255.255.255.0.

- A network/host policy object—Click **Select** to select an existing object or to create a new one. To use the object in this policy, it must have a single value, either a single network or a single host.

Configuring SNMP

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is a simple request/response protocol. The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap.

You can configure the sensor for monitoring by SNMP. SNMP defines a standard way for network management stations to monitor the health and status of many types of devices, including switches, routers, and sensors.

You can configure the sensor to send SNMP traps. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

Trap-directed notification has the following advantage—if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After receiving the event, the manager displays it and can take an action based on the event. For example, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Tip Trap-directed notification results in substantial savings of network and agent resources by eliminating frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent cannot send a trap if the device has had a catastrophic outage.

This procedure describes how to configure SNMP on an IPS sensor so that you can manage the sensor with an SNMP management station, including the configuration of traps.

Procedure

Step 1 Do one of the following to open the SNMP policy:

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Device Access > SNMP**, then select an existing policy or create a new one.

Step 2 On the **General Configuration** tab, configure at least the following options. For a complete description of all available options, see General SNMP Configuration Options , on page 11.

- **Enable SNMP Gets/Sets**—Select this option to enable the SNMP management workstation to obtain (get) information, and to modify (set) values on the IPS sensor. If you do not enable this option, the management workstation cannot manage this sensor.
- **Read-Only Community String**—The community string required for read-only access to the sensor. SNMP get requests from the management station must supply this string to get responses from the sensor. This string gives access to all SNMP get requests.
- **Read-Write Community String**—The community string required for read-write access to the sensor. SNMP set requests from the management station must supply this string to get responses from the sensor; it can also be used on get requests. This string gives access to all SNMP get and set requests.

Step 3 On the **SNMPv3 Users** tab, add one or more SNMPv3 users to configure SNMPv3 settings on the managed IPS devices. Beginning with version 4.6, Security Manager enables you to configure SNMPv3 settings on the IPS devices it manages. For more information, see SNMPv3 Users Tab , on page 12.

Note
SNMPv3 is supported in IPS version 7.2.2 and later, but not in the IPS version 7.3.1. Security Manager can however manage IPS 7.3.1 devices. If you try to use Security Manager to upgrade an IPS device from version 7.2.2, with SNMP policy configured, to version 7.3.1, a mouse-over tooltip displays the message "Selected upgrade is not recommended. Unassign the SNMP policy on the device and deploy it to continue with the upgrade to 7.3.1". For information about managing SNMPv3 policies on IPS devices with version 7.2.2 and later, see the Release Notes for Cisco Intrusion Prevention System 7.2(2).

Step 4 If you want to configure SNMP traps, click the **SNMP Trap Configuration** tab and configure at least the following options. For a complete description of all available options, see SNMP Trap Configuration Tab , on page 14.

- **Enable Notifications**—Select this option to allow the sensor to send SNMP traps.
- **Trap Destinations**—Add the SNMP management stations that should be trap destinations. Click the **Add Row (+)** button to add a new destination, or select a destination and click the **Edit Row (pencil)** button to change its configuration.

When adding or editing a trap destination, the trap community string that you enter overrides the default community string entered on the SNMP Trap Configuration tab. The community string appears in the traps sent to this destination and is useful if you are receiving multiple types of traps from multiple agents. For example, a router or sensor could be sending the traps, and if you put something that identifies the router or sensor specifically in your community string, you can filter the traps based on the community string.

To remove a destination, select it and click the **Delete Row (trash can)** button.

Step 5 If you configure trap destinations, you must also ensure that the desired alerts include the **Request SNMP Trap** action. You have the following options for adding this action:

- (Easy way.) Create an event action override to add the Request SNMP Trap action to all alerts of a specified risk rating (**IPS > Event Actions > Event Action Overrides** policy). For example, you could generate traps for all alerts with a risk rating between 85-100. Event action overrides let you add an action without individually editing each signature. For more information, see Configuring Event Action Overrides.
- (Precise way.) Edit the Signatures policy (**IPS > Signatures > Signatures**) to add the Request SNMP Trap action to the signatures for which you want to send trap notifications. Traps are sent only for signatures that you configure to send traps.

Note

If the signature has Default for the source, you have to change the source to the Local source before you can change the action. However, if you right-click the Action cell in the signatures table and select **Edit Actions**, then select Request SNMP Trap (along with any other desired action) and click **OK**, the source is automatically changed to Local.

Step 6 Add the SNMP management stations to the Allowed Hosts policy. The management stations must be allowed hosts to access the sensor. See Identifying Allowed Hosts , on page 8.

General SNMP Configuration Options

Use the General Configuration tab on the SNMP page to configure general SNMP parameters and apply them to IPS sensors. For the procedure, see Configuring SNMP , on page 9.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector. Select the General Configuration tab.
- (Policy view) Select **IPS > Platform > Device Admin > Device Access > SNMP**, then select an existing policy or create a new one. Select the General Configuration tab.

Field Reference

Table 1: General Configuration Tab, SNMP Policy for IPS Sensors

Element	Description
Enable SNMP Gets/Sets	Whether to enable the SNMP management workstation to obtain (get) information, and modify (set) values on the IPS sensor. If you do not enable this option, the management workstation cannot manage this sensor; the sensor will not respond to SNMP requests.
Read-Only Community String	The community string required for read-only access to the sensor. SNMP get requests from the management station must supply this string to get responses from the sensor. This string gives access to all SNMP get requests. Use the string to help identify the sensor.
Read-Write Community String	The community string required for read-write access to the sensor. SNMP set requests from the management station must supply this string to get responses from the sensor; it can also be used on get requests. This string gives access to all SNMP get and set requests. Use the string to help identify the sensor.
Sensor Contact	The network administrator or contact point who is responsible for this sensor.
Sensor Location	The physical location of the sensor, such as building address, name, and room number.

Element	Description
Sensor Agent Port	The port to use for SNMP get/set communication with the sensor. The default is 161. The valid range is 1 to 65535. Enter a port number or the name of a port list object, or click **Select** to select a port list object from a list or to create a new object. The port list object must identify a single port.
SNMP Agent Protocol	The protocol you are using for SNMP, either UDP (the default) or TCP. Select the protocol used by your SNMP management station.

SNMPv3 Users Tab

Beginning with version 4.6, Security Manager enables you to configure SNMPv3 settings on the IPS devices it manages. You must add SNMPv3 users to configure SNMPv3 settings on the managed IPS devices.

You can use the SNMPv3 Users tab on the SNMP page to view, add, edit, or delete SNMPv3 users.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector. Select the SNMPv3 Users tab.
- (Policy view) Select **IPS > Platform > Device Admin > SNMP**, then select an existing policy or create a new one. Select the SNMPv3 Users tab.

Do one of the following:

- To add an SNMPv3 user, click the **Add Row (+)** button. This opens the Add SNMPv3 User dialog box. Enter the information required to create the user. For detailed information on the settings, see Add SNMPv3 User Dialog Box , on page 13
- To edit an SNMPv3 user, select it and click the **Edit Row (pencil)** button and make the required changes in the Edit SNMPv3 User dialog box.
- To delete an existing SNMPv3 user, select it and click the **Delete Row (trash can)** button.

Field Reference

Table 2: SNMPv3 Users

Element	Description
User Name	Name of the user on the host that belongs to the SNMP agent.
Access Control	Access privilege for the SNMPv3 user.
Security Level	Security level for the SNMPv3 user.
Authentication Protocol	The authentication protocol keyword is the authentication level used to configure the SNMPv3 user.

Element	Description
Privacy Protocol	The privacy protocol keyword is the privacy or encryption algorithm used to configure the SNMPv3 user.

Add SNMPv3 User Dialog Box

Use the Add SNMPv3 User dialog box to configure a new SNMPv3 user for the managed IPS device.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector. Select the SNMPv3 Users tab and click the **Add Row (+)** button.
- (Policy view) Select **IPS > Platform > Device Admin > SNMP**, then select an existing policy or create a new one. Select the SNMPv3 Users tab and click the **Add Row (+)** button.

Field Reference

Table 3: Add SNMPv3 Users Dialog Box

Element	Description
User Name	Enter a name for the new SNMPv3 user.
Access Control	Select the access privilege for the new SNMPv3 user.
Security Level	Select one of the following security levels for the SNMPv3 user: • **NoAuthNoPriv**—There is no authentication and no privacy, which means that no security is applied to the messages. • **AuthNoPriv**—There is authentication but there is no privacy, which means that messages are authenticated. • **AuthPriv**—Authentication and privacy are configured, which means that messages are authenticated and encrypted.
Authentication Protocol	Select the authentication protocol keyword that specifies which authentication level should be used. There is no default value.
Privacy Protocol	Select the privacy protocol keyword that specifies which privacy or encryption algorithm should be used. For the encryption algorithm, you can specify the AES keyword. There is no default value.
Authentication Passphrase	Enter the authentication passphrase argument that specifies the authentication user password. This password must not be less than eight characters. There is no default value.
Privacy Passphrase	Enter the privacy passphrase argument that specifies the encryption user password. This password must not be less than eight characters. There is no default value.

SNMP Trap Configuration Tab

Use the SNMP Trap Communication tab on the SNMP page to configure traps and apply them to sensors and to identify recipients that the traps should be sent to. For the procedure, see Configuring SNMP , on page 9.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector. Select the SNMP Trap Configuration tab.
- (Policy view) Select **IPS > Platform > Device Admin > Device Access > SNMP**, then select an existing policy or create a new one. Select the SNMP Trap Configuration tab.

Field Reference

Table 4: SNMP Trap Configuration Tab, SNMP Policy for IPS Sensors

Element	Description
Enable Notifications	Whether to enable the sensor to send trap notifications to the trap destinations whenever a specific type of event occurs in a sensor. If you do not select this option, the sensor does not send traps. **Tip** To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures. Traps are sent only for signatures that you configure to send traps.
Error Filter	The type of events that will generate SNMP traps based on the severity of the event: fatal, error, or warning. Select all severities that you want; use Ctrl+click to select multiple values. The sensor sends notifications of events of the selected severities only.
Enable Detail Traps	Whether to include the full text of the alert in the trap. If you do not select this option, sparse mode is used. Sparse mode includes less than 484 bytes of text for the alert.
Default Trap Community String	The community string used for the traps if no specific string has been set for the trap destination in the Trap Destinations table. **Tip** All traps carry a community string. By default, all traps that have a community string identical to that of the destination are taken by the destination. All other traps are discarded by the destination. However, you can configure the destination to determine which trap strings to accept.

Element	Description
Trap Destinations table	The SNMP management stations that will be sent trap notifications. The table shows the IP address of the management station, the community string added to traps from this sensor, and the port to which traps are sent. • To add a destination, click the **Add Row** button and fill in the Add SNMP Trap Communication dialog box (see SNMP Trap Communication Dialog Box , on page 15). • To edit a destination, select it, click the **Edit Row** button and make your changes. • To delete a destination, select it and click the **Delete Row** button.

SNMP Trap Communication Dialog Box

Use the Add or Modify SNMP Trap Communication dialog box to configure SNMP trap destinations. These are the SNMP management stations that should receive traps from the IPS sensor.

Navigation Path

Go to the IPS **Platform > Device Admin > Device Access > SNMP** policy, select the **SNMP Trap Configuration** tab, and click the **Add Row** button beneath the Trap Destinations table, or select a destination in the table and click the **Edit Row** button. For more information, see SNMP Trap Configuration Tab , on page 14.

Field Reference

Table 5: SNMP Trap Communication Dialog Box

Element	Description
IP Address	The IP address of the SNMP management station that should receive trap notifications. Enter the IP address or the name of a network/host object, or click **Select** to select the object from a list or to create a new object. The network/host object must specify a single host IP address.
Trap Community String	The community string of the trap. If you do not enter a trap string, the default trap string defined on the SNMP Trap Communication tab is used for traps sent to this destination.
Trap Port	The port used by the SNMP management station to receive traps. Enter the port number or the name of a port list object, or click Select to select the object from a list or to create a new one. The port list object must identify a single port.
SNMPv3 User	Enter the username of the SNMPv3 user that you configured by using the Add SNMPv3 User Dialog Box , on page 13. Leave this field blank if you do not want to associate any SNMPv3 user. **Note** If you enter a username that is not a configured SNMPv3 user, you will receive an error message while trying to save the SNMP trap communication settings. () Also, note that you can add up to a maximum of 23 SNMPv3 users.

Managing User Accounts and Password Requirements

You can configure user accounts and passwords, and general password requirements, for your IPS devices. You can configure local users (defined directly on the device), use a RADIUS AAA server, or use them both in conjunction. The policies used are the **AAA**, **User Accounts**, and **Password Requirements** policies in the **Platform > Device Admin > Device Access** folder.

When you create or edit a local user account in Security Manager, the password you enter must satisfy the requirements defined in the Password Requirements policy. This ensures that new passwords meet your security requirements.

Tip If you change the password requirements, and then make changes to any local user account, the new requirements must be met by all user accounts that have passwords managed by Security Manager. This is because Security Manager reconfigures the passwords for all managed accounts if any single account needs to be reconfigured.

The User Accounts policy allows you to centrally manage the local user accounts for your IPS devices. Using a shared policy can help you ensure that all IPS devices contain the same accounts with the same passwords. However, it is important to understand that passwords are encrypted, so Security Manager cannot discover the actual passwords defined on the device. Security Manager manages the passwords for an account only if you define that password in Security Manager. Security Manager does not manage any user accounts defined in a RADIUS AAA server.

The following topics describe IPS user accounts, and Security Manager discovery and deployment considerations, in more detail:

- Understanding IPS User Roles , on page 16
- Understanding Managed and Unmanaged IPS Passwords , on page 17
- Understanding How IPS Passwords are Discovered and Deployed , on page 18
- Configuring IPS User Accounts , on page 19
- Configuring User Password Requirements , on page 21
- Configuring AAA Access Control for IPS Devices , on page 22

Understanding IPS User Roles

There are four user roles for IPS user accounts:

- **Viewer**—Users can view the device configuration and events, but they cannot modify any configuration data except their user passwords.
- **Operator**—Users can view everything and they can modify the following options:
  - Signature tuning (priority, disable or enable).
  - Virtual sensor definition.
  - Managed routers.

  - Their user passwords.

- **Administrator**—Users can view everything and they can modify all options that Operators can modify in addition to the following:
  - Sensor addressing configuration.
  - List of hosts allowed to connect as configuration or viewing agents.
  - Assignment of physical sensing interfaces.
  - Enable or disable control of physical interfaces.
  - Add and delete users and passwords.
  - Generate new SSH host keys and server certificates.
- **Service**—Only one user with service privileges can exist on a sensor. The service user cannot log in to IDM or IME. The service user logs in to a bash shell rather than the CLI. The service role is a special role that allows you to bypass the CLI if needed.

Note The purpose of the Service account is to provide Cisco Technical Support access to troubleshoot unique and unusual problems. It is not needed for normal system configuration and troubleshooting. You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Understanding Managed and Unmanaged IPS Passwords

Every IPS local user account has a password, which allows secure user login to the device. These user passwords are encrypted on the IPS device. Thus, when you add an IPS device to the Security Manager inventory, Security Manager cannot read the actual user passwords.

Because Security Manager cannot read the password, it is unable to deploy newly-discovered user account passwords to the device. To avoid putting user accounts into a state where the passwords are unknown and unusable, Security Manager marks discovered user account passwords as **unmanaged**. The status of a password is indicated in the **Is Password Managed?** column of the **Platform > Device Admin > Device Access > User Accounts** policy:

- If **No** is indicated, the password for this account is not configured in Security Manager. When you deploy this policy, Security Manager will not attempt to configure the password for this user account.
- If **Yes** is indicated, the password for this account was configured or updated in Security Manager. When you deploy this policy, Security Manager reconfigures the passwords for all managed accounts, not just the passwords that changed since the last deployment.

Because Security Manager configures even unchanged passwords, all managed passwords must satisfy the password requirements defined in the Password Requirements policy.

Thus, you can have a mix of managed and unmanaged account passwords. For example, you can have a set of shared user accounts that are centrally managed, and manage these account passwords in Security Manager.

Other accounts might be unique to individuals; if you never edit these account passwords in Security Manager, the user can manage these passwords individually on the device.

Tip If you do not want to manage any user accounts in Security Manager, ensure that the User Accounts policy is empty, or simply unassign the policy (right-click the policy and select **Unassign Policy**). Security Manager will not modify user account configurations.

Understanding How IPS Passwords are Discovered and Deployed

Because user passwords are encrypted on IPS devices, Security Manager has to handle them with special care when discovering policies on the device or deploying configurations. When discovering or deploying user accounts on IPS devices, Security Manager does the following:

- **Discovery**—When you add an IPS device to the inventory, or rediscover policies on it, Security Manager determines the current status of each user account, updates the User Account policy with each discovered username and associated role, and marks the user password as unmanaged (as described in Understanding Managed and Unmanaged IPS Passwords , on page 17).

You cannot view the account status through Security Manager, because it is dynamic and can change. However, the Discovery Status window displays the status at discovery. Accounts can have these statuses:

- **Active**—This state indicates that the account is available for use. Active accounts can be accessed using an authentication token if one has been assigned to the account.
- **Expired**—This state indicates that the account's authentication token has expired and the account can not be accessed using a token until the token has been updated.
- **Locked**—This state indicates that logins to the account have been disabled due to too many failed authentication attempts. You should update the password for these accounts.

Deployment—You are warned if any deployed user accounts are in the Expired or Locked state. Any unmanaged passwords are not deployed to the device. Also, keep in mind the following points:

- If you make changes to any user account on the device, all user accounts with managed passwords are reconfigured. If you also changed the Password Requirements policy, all passwords are compared to the new policy and must meet the new requirements.
- If you change the password of the user account you defined in the device's properties for Security Manager to use when configuring the device, after successful deployment, Security Manager updates the password in the device properties to the new password. You do not need to manually update the password. To see device properties, select **Tools > Device Properties**.

This behavior assumes that you selected **Security Manager Device Credentials** for the Connect to Device Using option on the **Tools > Security Manager Administration > Device Communication** page. If you are using the logged-in users credentials for deployment, after successful deployment, the overall deployment is marked as failed, and a message explains how to reestablish connection. See Device Communication Page.

- If you use out-of-band change detection, changes to passwords are not detected. However, changes to usernames and roles are detected. For more information about out-of-band change detection, see Detecting and Analyzing Out of Band Changes.

- When previewing configurations, you can see changes to the user accounts by selecting to IPS(Delta – User Passwords). However, passwords are masked. For more information, see Previewing Configurations.
- If you are rolling back configurations, the user accounts are never rolled back. The current status and configuration of user accounts does not change.

Tip The IPS sensor can accept public keys for RSA authentication when logging into the device through an SSH client. Each user has an associated list of authorized keys. Users can use these keys instead of passwords. Security Manager ignores these keys during discovery and deployment. Thus, if keys are configured, Security Manager does not remove the configuration.

Related Topics

- Discovering Policies
- Deploying Configurations in Non-Workflow Mode
- Deploying Configurations in Workflow Mode
- Understanding Configuration Rollback
- Understanding Rollback for IPS and IOS IPS

Configuring IPS User Accounts

Use the User Accounts policy to configure local user accounts for IPS devices. Users can use these accounts to log into the device. You can create new users, modify user privileges and passwords, and delete users.

The user accounts policy should have at least these accounts:

- cisco—An account named “cisco” must exist on the device and you cannot delete it.
- An administrator account that Security Manager can use—Security Manager must be able to log into the device to configure it. Typically, you create an account for this purpose. However, you have the option of having Security Manager use the user account of the person deploying configurations to log into the device. You can configure this using the **Connect to Device Using** option on the **Tools > Security Manager Administration > Device Communication** page. See Device Communication Page.

IPS user account configuration is more complicated than it seems. Before you configure IPS user accounts, read the following topics:

- Managing User Accounts and Password Requirements , on page 16
- Understanding IPS User Roles , on page 16
- Understanding Managed and Unmanaged IPS Passwords , on page 17
- Understanding How IPS Passwords are Discovered and Deployed , on page 18
- Configuring User Password Requirements , on page 21
- Configuring AAA Access Control for IPS Devices , on page 22

Tips

- Cisco IOS IPS devices use the same user accounts that are defined for the router. This procedure does not apply to Cisco IOS IPS configurations.
- If you change the password for the user defined in the device properties, which Security Manager uses to deploy configurations to the device, Security Manager uses the existing credentials defined in the device properties to log into the device and deploy changes. After successful deployment, the device properties are then changed to use your new settings. For more information on credentials in device properties, see Device Credentials Page.

Related Topics

- Filtering Tables
- Table Columns and Column Heading Features

Procedure

Step 1 Do one of the following to open the User Accounts policy:

- (Device view) Select **Platform > Device Admin > Device Access > User Accounts** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Device Access > User Accounts**, then select an existing policy or create a new one.

The policy shows existing user accounts, including the username, role, and whether the password is managed by Security Manager (as explained in Understanding Managed and Unmanaged IPS Passwords , on page 17).

Step 2 Do one of the following:

- To add a user account, click the **Add Row (+)** button. This opens the Add User dialog box. Enter the information required to define the account. For detailed information on the settings, see Add User and Edit User Credentials Dialog Boxes , on page 21.
- To edit a user account, select it and click the **Edit Row (pencil)** button and make the required changes in the Edit User dialog box.

You cannot change a user role to or from the Service role.

- To delete a user account, select it and click the **Delete Row (trash can)** button. You cannot delete the account named cisco.

Tip
All password changes must meet the requirements of the Password Requirements policy. If you change the requirements policy, all new user accounts, or edited accounts, are tested against the new requirements. Although the passwords for existing unedited user accounts are not tested, they too must meet the password requirements if you change any user account defined in this policy, because Security Manager will deploy all of the accounts during the next configuration deployment. Passwords are checked for conformity when you validate policies, which typically happens when you submit changes to the database. For more information, see Understanding How IPS Passwords are Discovered and Deployed , on page 18.

Add User and Edit User Credentials Dialog Boxes

Use the Add User or Edit User Credentials dialog boxes to add or edit IPS device user accounts.

Navigation Path

From the IPS platform User Accounts policy, click the **Add Row (+)** button to create a new account, or select an existing account and click the **Edit Row (pencil)** button. For information on accessing the User Accounts policy, see Configuring IPS User Accounts , on page 19.

Field Reference

Table 6: Add or Edit User Dialog Box

Element	Description
User Name	The username for the account. The name can be 1 to 64 characters, including uppercase and lowercase letters and numbers, plus the special characters ( ) + : , _ / -] + $. You cannot change the username when editing an account.
Password Confirm	The password for this user account. Enter the password in both fields. The password must conform to the Password Requirements policy for IPS devices; see Configuring User Password Requirements , on page 21.
Role	The role for this user. For an explanation of these roles, see Understanding IPS User Roles , on page 16. **Tip** When editing a user account, you cannot select the Service role. When editing an account assigned to the Service role, you cannot change the role.

Configuring User Password Requirements

Use the IPS platform Password Requirements policy to configure the rules for passwords for local IPS device user accounts. All user-created sensor passwords must conform to the requirements defined in this policy. You can configure password requirements for sensor running IPS software version 6.0 or later.

Tip The requirements you define here determine what is considered an acceptable password in the User Accounts policy (see Configuring IPS User Accounts , on page 19). If you change this policy, it can be applied even to unchanged user accounts. For more information about the implications of deploying changes to this policy, see Understanding How IPS Passwords are Discovered and Deployed , on page 18.

To configure IPS password requirements, select one of the following policies:

- (Device view) Select **Platform > Device Admin > Device Access > Password Requirements** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Password Requirements** from the Policy Type selector, then select an existing policy or create a new one.

The following table explains the password requirement options that you can configure.

Table 7: Password Requirements Policy

Element	Description
Attempt Limit	How many times a user is allowed to try to log into the device before you lock the user account due to excessive failed attempts. The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.
Size Range	The minimum and maximum size allowed for user passwords; separate the minimum and maximum with a hyphen. The range is 6 to 64 characters; the default is 8-64. **Tip** If you configure non-zero values for any of the minimum characters options, the minimum size you enter in the Size Range field must be equal to or greater than the sum of those values. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.
Minimum Digit Characters	The minimum number of numeric digits that must be in a password.
Minimum Uppercase Characters	The minimum number of uppercase alphabet characters that must be in a password.
Minimum Lowercase Characters	The minimum number of lowercase alphabet characters that must be in a password.
Minimum Other Characters	The minimum number of non-alphanumeric printable characters that must be in a password.
Number of Historical Passwords	The number of historical passwords that you want the sensor to remember for each account. Any attempt to change the password of an account fails if the new password matches any of the remembered passwords. If you specify 0, no previous passwords are remembered.

Configuring AAA Access Control for IPS Devices

Use the AAA policy to configure AAA access control for your IPS devices. The device must use IPS Software release 7.0(4) or above or 7.1.3 or above to configure AAA; for example, neither 7.1.1 nor 7.1.2 supports AAA.

You can configure the IPS device to use a RADIUS AAA server to authenticate user access to the device. By configuring AAA, you can reduce the number of local users defined on the device and take advantage of your existing RADIUS setup. If you configure a AAA server, you can configure the device to allow local user accounts as a fallback mechanism if the RADIUS servers are unavailable.

When configuring AAA, you identify the RADIUS server using a AAA server policy object. You can create the object while configuring the policy, or you can create it in the Policy Object Manager. When you configure the AAA server object, you must adhere to the following restrictions:

- **Host**—You must specify the IP address; you cannot use a DNS name.
- **Timeout**—If you enter a timeout value, it must be from 1 to 512 seconds. The generic AAA server object allows higher numbers, but IPS has a more limited timeout range. The default is 3.
- **Protocol**—RADIUS is the only supported protocol.
- **Key**— You must specify the shared secret key that is defined on the RADIUS server. Although this field is optional for a generic AAA server object, IPS requires a key.
- **Port**—Ensure that the RADIUS Authentication/Authorization port is correct. Note that the default port in the AAA server object is different from the IPS default, which is 1812. You will need to change the port if you want to use the IPS default.

For more information about configuring AAA server objects, see Creating AAA Server Objects.

Tip You must ensure that the user account configured in the device properties exists in the RADIUS server or as a local user account, depending on the authorization method that you use. If you switch between local and AAA modes, or change AAA servers, you must ensure that the account is defined in whatever user account database you are using. If you are using AAA with local fallback, the account should be defined in all databases. This account must exist, with the same password defined in the Security Manager device properties for the device, or deployment to the device will fail. The user account used for discovery and deployment must have administrator privileges.

Related Topics

- Managing User Accounts and Password Requirements , on page 16
- Configuring IPS User Accounts , on page 19

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **Device Access** > **AAA** from the Policy selector.
- (Policy view) Select **IPS** > **Platform** > **Device Admin** > **AAA**, then select an existing policy or create a new one.

Step 2 Configure the following basic properties:

- **Authentication Mode**—Whether to use Local or AAA mode. Local mode uses user accounts defined on the IPS device only. With AAA mode, the RADIUS servers are the primary means of user authentication, and you can configure local user accounts as a fallback mechanism. The default is Local. You must select AAA to configure any other options in this policy.
- **Primary RADIUS Server, Secondary RADIUS Server**—The main (primary) AAA server and a backup server, if any. Enter the name of the AAA server policy object that identifies the RADIUS server, or click **Select** to select it from a list of objects or to create a new object.

When authenticating users, the IPS device sends the user authentication attempt to the primary server. The secondary server is contacted only if the request to the primary server times out.

Step 3 Configure the following optional properties if you want non-default values:

- **Console Authentication**—How you want to authenticate users who access the IPS device through the console:
  - Local—Users connected through the console port are authenticated through local user accounts.
  - Local and RADIUS—Users connected through the console port are authenticated through RADIUS first. If RADIUS fails, local authentication is attempted.
  - RADIUS—Users connected through the console port are authenticated by RADIUS. If you also select Enable Local Fallback, then users can also be authenticated through the local user accounts.
- **RADIUS NAS ID**—The Network Access ID, which identifies the service requesting authentication. The value can be no NAS-ID, cisco-ips, or a NAS-ID already configured on the RADIUS server. The default is cisco-ips.
- **Enable Local Fallback**—Whether you want to fall back to local user account authentication if all RADIUS servers are unavailable. This option is selected by default. Note that local authentication is not attempted if the RADIUS server responds negatively to the logon attempt; local authentication is tried only if no response is received from the RADIUS server.
- **Default User Role**—The role to assign to users who do not have a role assigned in the RADIUS server. You can make Viewer, Operator, or Administrator the default roles, but not Service; select Unspecified to assign no default role (this is the default). For an explanation of user roles, see Understanding IPS User Roles , on page 16.

Note
User role configuration is very important. If you do not assign a role to the user, either through the default user role or in the RADIUS server, the sensor prevents user login even if the RADIUS server accepted the username and password.

To assign roles specifically to users on the RADIUS server, you configure the Accept Message for those accounts as either ips-role=administrator, ips-role=operator, ips-role=viewer, or ips-role=service. You configure the Accept Message individually for each user account. An example of a Reply attribute for a given user could be configured to return “Hello <user> your ips-role=operator.”

If you configure a service account in the RADIUS server, you must also configure an identical service account locally on the device. For service accounts, both the RADIUS and Local accounts are checked during login.

Identifying an NTP Server

Use the NTP policy to configure a Network Time Protocol (NTP) server as the time source for the IPS device. Using NTP helps ensure synchronized time among your network devices, which can aid event analysis. NTP is the recommended way to configure time settings on an IPS device.

For detailed information on how to set the time on a sensor, including how to set up a Cisco IOS router as an NTP server, refer to Configuring Time in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface Version 7.0* .

Tip Check the time on your IPS sensor if you are having trouble updating your IPS software. If the time on the sensor is ahead of the time on the associated certificate, the certificate is rejected, and the sensor software update fails.

Procedure

Step 1 Do one of the following to open the NTP policy:

- (Device view) Select **Platform** > **Device Admin** > **Server Access** > **NTP** from the Policy selector.
- (Policy view) Select **IPS** > **Platform** > **Device Admin** > **Server Access** > **NTP**, then select an existing policy or create a new one.

Step 2 In the **NTP Server IP Address** field, enter the IP address of the NTP server. You can also enter the name of a network/host object that identifies the single host address of the server, or click **Select** to select the object from a list or to create a new one.

Note
Beginning with Cisco Security Manager 4.19, you can configure NTP server with IPV6 address for all ASA 9.12(1) and later devices.

Step 3 If the NTP server does not require authentication, deselect the **Authenticated NTP** checkbox.

If the NTP server requires authentication, configure the following options:

- **Authenticated NTP**—Select this option to enable authenticated connections.
- **Key, Confirm**—The key value of the NTP server. The key is an MD5 type of key (either numeric or character); it is the key that was used to set up the NTP server.
- **Key ID**—The key ID value of the NTP server, a numeric value between 1 and 65535.

Tip
The key and key ID are configured on the NTP server; you must obtain them from the NTP server configuration.

Identifying DNS Servers

If you configure global correlation on an IPS 7.0+ sensor, the sensor must be able to resolve domain names to successfully connect to the update server when downloading global correlation updates. Use the DNS policy to identify the Domain Name System (DNS) servers that the sensor can use to resolve domain names to IP addresses.

Tip If your network requires HTTP proxies when making Internet connections, configure the HTTP Proxy policy instead of the DNS policy. See Identifying an HTTP Proxy Server , on page 26.

Note The AIP-SSC-5 service module does not support DNS servers.

Procedure

Step 1 Do one of the following to open the HTTP Proxy policy:

- (Device view) Select **Platform > Device Admin > Server Access > DNS** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Server Access > DNS**, then select an existing policy or create a new one.

Step 2 Specify the IP addresses of up to three DNS servers in the **Primary, Secondary, and Tertiary Address** fields. The sensor uses the servers in the order listed; if one server does not respond, the next server is contacted.

You can enter an IP address or the name of a network/host object that contains a server address. Click **Select** to select a network/host object from a list or to create a new one. The network/host object must specify a single host address.

Identifying an HTTP Proxy Server

If you configure global correlation on an IPS 7.0+ sensor, and your network requires the use of HTTP proxies to connect to the Internet, you need to configure the HTTP Proxy policy to identify a proxy that the IPS sensor can use. When downloading global correlation updates, the IPS sensor connects to the update server using this proxy. The proxy must be able to resolve DNS names.

Tip If you do not use HTTP proxies, configure DNS servers so that the IPS sensor can resolve the address of the update server. See Identifying DNS Servers , on page 25.

Note The AIP-SSC-5 service module does not support HTTP proxy servers.

Procedure

Step 1 Do one of the following to open the HTTP Proxy policy:

- (Device view) Select **Platform > Device Admin > Server Access > HTTP Proxy** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Server Access > HTTP Proxy**, then select an existing policy or create a new one.

Step 2 Configure the following options:

- **Enable Proxy**—Select this option to tell the device to connect through the configured proxy server.
- **IP Address**—Enter the IP address of the proxy server, or the name of the network/host object that contains the server's IP address. Click **Select** to select a network/host object from a list or to create a new one. The network/host object must contain a single host IP address.

- **Port**—Enter the port number used for HTTP connections to the proxy server. The default is 80.

IPS SSHv2 Known Host Keys

The IPS SSHv2 Known Host Keys policy enables you to configure SSHv2 server host keys (outgoing SSHv2 connections from an IPS sensor to an SSH server). This feature is available on IPS sensors running 7.1(8) and later versions of Cisco IPS.

The host key can be retrieved from an IPS sensor using valid IP addresses; alternatively, it can be entered manually if you know it. The host key retrieval may take few seconds.

Procedure

Step 1 Do one of the following to open the IPS SSHv2 Known Host Keys policy:

- (Device view) Select **Platform** > **Device Admin** > **Server Access** > **SSHv2 Known Host Keys** from the Policy selector.
- (Policy view) Select **IPS** > **Platform** > **Device Admin** > **Server Access** > **SSHv2 Known Host Keys**, then select an existing policy or create a new one.

Step 2 Click the **Add** button to open the Add or Edit Known Host RSA Key Dialog Box, on page 27.

Step 3 Select a row and then click the **Edit** button to open the Add or Edit Known Host RSA Key Dialog Box, on page 27.

Add or Edit Known Host RSA Key Dialog Box

Use the Add or Edit Known Host RSA Key dialog box to retrieve an SSHv2 key from an IPS sensor or to enter the key manually if you know it.

Navigation Path

From the SSHv2 Known Host Keys policy, click the **Add** button beneath the IP Address/Public Key table, or select a row in the table and click the **Edit** button. For information on the SSHv2Known Host Keys policy, see IPS SSHv2 Known Host Keys, on page 27.

Field Reference

Table 8: Add or Edit Known Host RSA Key Dialog Box

Element	Description
IP Address	The IP address of the IPS sensor from which you want to retrieve the public key.

Element	Description
Retrieve Public Key	Initiates retrieval of the public key from the device identified in the IP Address field. The Retrieve Public Key option is available in device view (it is not shown in shared policy view). However, you can enter inline values for the public key in shared policies or retrieve the public key in device view and share it using the "share policy" option.
Public Key	The public key that you know and are able to enter manually. For shared policies, you will be able to enter inline values for the host key.

Configuring IPS SSHv1 Fallback Settings

The IPS SSHv1 Fallback policy is available on IPS sensors running 7.1(8) and later versions of Cisco IPS.

Procedure

Step 1 Do one of the following to enable or disable SSHv1 Fallback:

- (Device view) Select **Platform > Device Admin > Server Access >Settings** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Server Access > Settings**, then select an existing policy or create a new one.

Step 2 To enable SSHv1 fallback, click the checkbox.

Step 3 To disable SSHv1 fallback, clear the checkbox.

Configuring the External Product Interface

Use the External Product Interface policy to configure the way that Security Manager works with Management Center for Cisco Security Agents (CSA MC).

In general, the external product interface is designed to receive and process information from external security and management products. These external security and management products collect information that can be used to automatically enhance the sensor configuration information. Management Center for Cisco Security Agents is the only external product that can be configured to communicate with the IPS. At most two Management Center for Cisco Security Agents servers can be configured per IPS device.

Tip Management Center for Cisco Security Agents is no longer an active product. Configure this policy only if you are still using that application. For more information, see About CSA MC in *Installing and Using Cisco Intrusion Prevention System Device Manager 6.0* and http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html.

Management Center for Cisco Security Agents enforces a security policy on network hosts. It has two components:

- Agents that reside on and protect network hosts.
- A management console, which is an application that manages agents. It downloads security policy updates to agents and uploads operational information from agents.

Before You Begin

Add the external product as an allowed host so that Security Manager allows the sensor to communicate with the external product. For more information, see Identifying Allowed Hosts , on page 8.

Procedure

Step 1 Do one of the following to open the External Product Interface policy:

- (Device view) Select **Platform > Device Admin > Server Access > External Product Interface** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Server Access > External Product Interface**, then select an existing policy or create a new one.

The **Management Center for Cisco Security Agents** tab shows any existing definitions, including the IP address (or network/host object), URL, and port of the external application, the username and password used to log into it, and whether the connection is enabled. The interface type is always Extended SDEE.

Step 2 Do one of the following:

- To add a server, click the **Add Row (+)** button. This opens the External Product Interface dialog box. Enter the information required to identify the server and configure the posture ACLs. For detailed information on the settings, see External Product Interface Dialog Box , on page 29.

You can add at most two servers.

- To edit a server, select it and click the **Edit Row (pencil)** button and make the required changes in the External Product Interface dialog box.
- To delete a server, select it and click the **Delete Row (trash can)** button.

External Product Interface Dialog Box

Use the Add or Edit External Product Interface dialog box to add or modify interfaces between Management Center for Cisco Security Agents (CSA MC) and the IPS device and the related posture ACLs.

Navigation Path

From the External Product Interface IPS platform policy, click **Add Row** or select an entry and click **Edit Row**. For information on opening the External Product Interface policy, see Configuring the External Product Interface , on page 28.

Field Reference

Table 9: External Product Interface Dialog Box

Element	Description
External Product's IP Address	The IP address, or the network/host policy object that contains the address, of the external product. Enter the IP address or object name, or click **Select** to select an object from a list or to create a new one.
Interface Type	Identifies the physical interface type, which is always Extended SDEE.
Enable receipt of information	Whether information is allowed to be passed from the external product to the sensor.
SDEE URL	The URL on the CSA MC the IPS uses to retrieve information using SDEE communication. You must configure the URL based on the software version of the CSA MC that the IPS is communicating with as follows: • For CSA MC version 5.0—/csamc50/sdee-server. • For CSA MC version 5.1—/csamc51/sdee-server. • For CSA MC version 5.2 and later—/csamc/sdee-server (the default value).
Port	The port, or the port list object that identifies the port, being used for communications. Enter the port or port list name, or click **Select** to select the object from a list or to create a new object.
User name Password	A username and password that can log into the external product.
Enable receipt of host postures	Whether to allow the receipt of host posture information from CSA MC. The host posture information received from a CSA MC is deleted if you disable this option.
Allow unreachable hosts' postures	Whether to allow the receipt of host posture information for hosts that are not reachable by the CSA MC. A host is not reachable if the CSA MC cannot establish a connection with the host on any IP addresses in the host's posture. This option is useful in filtering the postures whose IP addresses may not be visible to the IPS sensor or that might be duplicated across the network. This filter is most applicable in network topologies where hosts that are not reachable by the CSA MC are also not reachable by the IPS, for example if the IPS and CSA MC are on the same network segment.

Element	Description
Posture ACL table	Posture ACLs are network addresses for which host postures are allowed or denied. Use posture ACLs to filter postures that have IP addresses that might not be visible to the IPS or that might be duplicated across the network. • To add a posture ACL, click the **Add Row (+)** button. This opens the Add Posture ACL dialog box. For information on configuring the Posture ACL, see Posture ACL Dialog Box , on page 31. • To edit a posture ACL, select it and click the **Edit Row (pencil)** button. • To delete a posture ACL, select it and click the **Delete Row (trash can)** button. • To change the priority of an ACL, select it and click the Up or Down button. ACLs are processed in order, and the action associated with the first match is applied.
Enable receipt of watch listed addresses	Whether to allow the receipt of the watch list information from CSA MC. The watch list information received from a CSA MC is deleted if you disable this option.
Manual Watch List RR increase	The percentage of the manual watch list risk rating (RR). The default is 25, and the valid range is 0 to 35.
Session-based Watch List RR Increase	The percentage of the session-based watch list risk rating. The default is 25, and the valid range is 0 to 35.
Packed-based Watch List RR Increase	The percentage of the packet-based watch list risk rating. The default is 10, and the valid range is 0 to 35.

Posture ACL Dialog Box

Use the Add or Modify Posture ACL dialog box to configure posture ACLs for Management Center for Security Agents. Posture ACLs are network addresses for which host postures are allowed or denied. Use posture ACLs to filter postures that have IP addresses that might not be visible to the IPS or that might be duplicated across the network.

Configure the following fields to define a posture ACL:

- **Network Address**—Enter the IP address of a host or network, or the name of a network/host object that specifies one. You can click **Select** to select the object from a list or to create a new object.
- **Action**—Whether host postures will be permitted or denied from the hosts on the network address.

Navigation Path

From the External Product Interface dialog box (see External Product Interface Dialog Box , on page 29), click the **Add Row (+)** button underneath the Posture ACL table, or select a posture ACL and click the **Edit Row (pencil)** button.

Configuring IPS Logging Policies

Use the IPS platform Logging policy to configure traffic flow notifications and Analysis Engine global variables. These settings apply to the general operation of the IPS sensor.

Traffic flow notifications have to do with the flow of traffic across the interface of a sensor. You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts and stops) during a specified interval. You can configure the missed packet threshold within a specific notification interval and also configure the interface idle delay before a status event is reported.

The Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces. For the Analysis Engine, there is only one global variable: Maximum Open IP Log Files.

Navigation Path

- (Device view) Select **Platform > Logging** from the Policy selector.
- (Policy view) Select **IPS > Platform > Logging**, then select an existing policy or create a new one.

Field Reference

Table 10: IPS Logging Page

Element	Description
Interface Notifications Tab	
Missed Packets Threshold	The percent of missed packets that has to occur before you want to receive notification. The default is 0, and the range is 0 to 100.
Notification Interval	The length of time, in seconds, that you want to check for the percentage of missed packets. The default is 30, and the range is 5 to 3600.
Interface Idle Threshold	The length of time, in seconds, that you will allow an interface to be idle and not receiving packets before you want to be notified. The default is 30, and the range is 5 to 3600.
Analysis Engine Tab	
Specify-Flow-Depth	Lets you specify the inspection depth of the flow. Flow depth is the number of bytes inspected in a flow. The new value applies for new flows only. The valid range is from 0 to 429496296. The default is 0.
Enable Service Activity	Service activity lets you gather information about service activities for diagnostic purposes. The details are more granular and have port level details. Enabling service activity impacts system performance. Enable service activity collection temporarily for diagnostic purposes only. You must reboot the sensor after you enable service activity for the change to take effect.
Service Activity Limit	Sets the limit for how many services you want to enable. The valid range is from 10 to 65536. The default is 15.

Element	Description
Note The Specify-Flow-Depth, Enable Service Activity, and Service Activity Limit fields are applicable to IPS devices of version 7.2(2) or later.	
Maximum Open IP Log Files	The maximum number of open IP log files that you want to allow on the sensor. The default is 20, and the range is 20 to 100.

IPS Health Monitor

Use the IPS Health Monitor page to configure the metrics, or parameters, that are used to determine the health and network security status of your IPS devices. Your IPS devices use these metrics to assign appropriate severity when sending IPS events. The results appear in the Health and Performance Monitor of Security Manager (Launch > Health and Performance Monitor).

IPS Health Monitor is supported in IPS devices beginning with IPS version 6.1 and in Security Manager beginning with version 4.4. Please note the following special cases:

1. For IPS devices running 7.x, all 11 configuration items in the IPS Security Settings Policy are displayed and monitored properly in the Security Manager GUI.
2. For IPS devices running less than 6.1, the Network Participation and Global Correlation entries are hidden in the device view of Security Manager.
3. Some IPS Health Monitor configuration items are protected entries on the device side itself and cannot be edited. Security Manager informs you in such cases.

If you do not select a metric by checking the check box, it does not appear in the Health and Performance Monitor. You can accept the default configuration or edit the values. Items will be disabled and will not be editable if you do not select a metric.

The overall health is set to the most critical settings of any of the metrics. For instance, if all the selected metrics are normal except for one that is critical, the overall health becomes critical. The IPS sensor sends a health and security status event when the overall health status of the IPS sensor changes.

The security status of the IPS sensor is determined for each virtual sensor using the threat ratings of events detected by the virtual sensors. The security status of the virtual sensor is raised when the virtual sensor detects an event with a threat rating that exceeds the threshold for that virtual sensor. After a threshold has been exceeded, the security status remains at a critical level until the configured amount of time has passed with no more events being detected at the higher level.

To configure the metrics on the IPS Health Monitor page, select one of the following policies:

- (Device view) Select **Platform > Device Admin > Health Monitor** from the Policy selector.
- (Policy view) Select **IPS > Platform > Device Admin > Health Monitor** from the Policy Type selector, then select an existing policy or create a new one.

Note In policy view, no validation is performed if a shared IPS Health Monitor policy is applied to an IPS device running less than 6.1. Security Manager ignores such policies during deployment to device and captures them in deployment logs also.

The following table explains the IPS Health Monitor Metrics that you can configure.

Table 11: IPS Security Settings Policy

Element	Description
Inspection Load	Lets you set a threshold for inspection load and whether this metric is applied to the overall sensor health rating.
Missed Packet	Lets you set a threshold percentage for missed packets and whether this metric is applied to the overall sensor health rating.
Memory Usage	Lets you set a threshold percentage for memory usage and whether this metric is applied to the overall sensor health rating.
Signature Update	Lets you set a threshold for when the last signature update was applied and whether this metric is applied to the overall sensor health rating.
License Expiration	Lets you set a threshold for when the license expires and whether this metric is applied to the overall sensor health rating.
Event Retrieval	Lets you set a threshold for when the last event was retrieved and whether this metric is applied to the overall sensor health rating. **Note** The event retrieval metric keeps track of when the last event was retrieved by an external monitoring application such as IME. Disable Event Retrieval if you are not doing external event monitoring.
Network Participation	Lets you choose whether the Network Participation health metrics contribute to the overall sensor health rating.
Global Correlation	Let you choose whether the Global Correlation health metrics contribute to the overall sensor health rating.
Application Failure	Lets you choose to have an application failure applied to the overall sensor health rating.
IPS in Bypass Mode	Let you choose to know if bypass mode is active and have that apply to the overall sensor health rating.
One or More Active Interfaces Down	Lets you choose to know if one or more enabled interfaces are down and have that apply to the overall sensor health rating.
Warning	Lets you set the lowest threshold in percentage, days, seconds, or failures for the warning threshold.
Critical	Lets you set the lowest threshold in percentage, days, seconds, or failures for the critical threshold.

Configuring IPS Security Settings

Use the IPS Security Settings policy to configure two items that are important to the security of your IPS devices:

- **Permit packet capture logging**—With this feature, IPS devices can prevent users from arbitrarily executing packet capture/display/iplog commands. In previous versions of Security Manager, such actions leave no trace of who executed the command.
- **Configurable idle timeout**—When configured, this feature terminates the connection to an IPS device after a period of time that you specify. Its purpose is to increase the security of a CLI session.

Note These settings are available for devices operating with IPS 7.1.3 and later.

To configure IPS security settings, select one of the following policies:

- (Device view) Select **Platform > Security >Settings** from the Policy selector.
- (Policy view) Select **IPS > Platform > Security > Settings** from the Policy Type selector, then select an existing policy or create a new one.

The following table explains the IPS security settings that you can configure.

Table 12: IPS Security Settings Policy

Element	Description
Permit packet logging	Whether to enable packet logging; applies to packet capture/display/iplog commands.
CLI Inactivity Timeout (In Minutes)	Terminates the connection to an IPS device after the specified period of time.