



CHAPTER 8

IPS

This chapter contains the following topics:

- [Importing IPS 5.0 Sensors, page 8-1](#)
- [Retrieving Signature Updates, page 8-1](#)
- [Performing IPS Updates, page 8-2](#)
- [Updating IOS IPS Crypto Configurations, page 8-2](#)
- [Creating ACLs During IOS IPS Configuration, page 8-3](#)
- [Performing IOS IPS Deployment, page 8-3](#)
- [Provisioning Trusted Hosts, page 8-3](#)
- [Managing Signature Updates, page 8-3](#)



Note

For more detailed information see the “Managing IPS Devices” chapter in the [User Guide for Cisco Security Manager](#) for your release.

Importing IPS 5.0 Sensors

Problem You cannot import IPS 5.0 (or earlier) sensors into Security Manager.

Solution Version 3.2 of Security Manager supports IPS 5.1, IPS 6.0, and IPS-enabled IOS 12.4(11)T2 and above only. When you import a sensor on which virtual sensors are configured, you must submit your changes (or approve your activity when working in Workflow mode) after discovery in order to view the virtual sensors in the Device selector. A warning message that explains this is displayed after discovery.

Retrieving Signature Updates

Problem You cannot connect to the Update Server or CCO to retrieve signature updates into Security Manager.

Solution Make sure that you have specified the location from which Security Manager should download signature updates. Select **Tools > Security Manager Administration > IPS Updates**, then click **Edit Settings** under Update Server to enter this information. After updating the server information, make sure you click **Save** at the bottom of the page.

Performing IPS Updates

Problem You cannot update your IPS sensor with patches, service packs, or signature updates.

Solution Check the time on your IPS sensor. If the time on the sensor is ahead of the time on the associated certificate, the certificate is rejected and the update may fail. Use the Network Time Protocol (NTP) to maintain accurate time on an IPS sensor.

The following procedures describes how to identify an NTP server.



Caution

If your sensors already have an NTP server configuration, you must identify the NTP server by performing the relevant procedure. Otherwise, your NTP server settings are lost.



Note

Signature updates are available for IPS 5.1(4) and above.

- Step 1** In Device view, select the IPS sensor for which you want to identify an NTP server.
- Step 2** Select **Platform > Device Admin > Server Access > NTP**. The Network Time Protocol page appears.
- Step 3** In the NTP Server IP Address field, enter the address of the NTP server.
- Step 4** In the Key field, enter the key value of the NTP server.
- Step 5** In the Key ID field, enter the key ID value of the NTP server. Valid values are 1 through 4294967295.
- Step 6** Click **Save** to save your definitions to the Security Manager server.



Note

To publish your changes, click the **Submit** button on the toolbar.



Note

For detailed information on how to set the time on a sensor, refer to [Configuring the Sensor to Use an NTP Time Source](#) in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0*, which is available on Cisco.com. You will be prompted for your CCO username and password.

Updating IOS IPS Crypto Configurations

Problem You cannot update your IOS IPS Crypto configuration.

Solution Check whether the TFTP server is running on your Cisco Security Manager server. Make sure your TFTP directory has the required permissions to enable IOS IPS to download the certificate from it. The default TFTP directory for Windows 2000 and 2003 is `<install-dir>\tftpboot`. In addition, you must have a user account with adequate privileges to update IOS IPS crypto configurations.

Creating ACLs During IOS IPS Configuration

Problem ACL creation during IOS IPS configuration is not producing the expected results.

Solution Entering the name or number of an ACL on the following IPS Manager pages does not actually create the ACL:

- IOS IPS Rules page
- IOS IPS Filters page
- IOS IPS Port Mapping page

To create the ACL, use the command line on the IOS IPS device that you are configuring. If you enter an ACL number and deploy the configuration while no corresponding ACL exists in the router, this command has no effect.

Performing IOS IPS Deployment

Problem You receive an error message during initial deployment of an IOS IPS device.

Solution You may have exceeded the memory available on the IOS IPS device. To work around this problem, select a reduced set of signatures to be deployed and then redeploy the IOS IPS device.

Provisioning Trusted Hosts

Problem You cannot provision a Management Center for Cisco Security Agent (CSA MC) server as a trusted host to an IPS sensor.

Solution You must use CLI commands or the IPS Device Manager (IDM). When you add a CSA MC server to an IPS sensor in IDM, a message appears that asks whether to add the server as a trusted host to the sensor. (There is a separate option in IDM for adding a list of IP addresses as trusted hosts to the sensor.)

Managing Signature Updates

Problem You cannot obtain signature updates for a sensor running IPS 5.1.

Solution Although Security Manager supports IPS 5.1 and above, signature updates are available only for IPS 5.1(4) and IPS 6.0.

