Managing IPS Sensors

To perform day-to-day sensor management, you typically need to use a device manager such as the IPS Device Manager (IDM). Security Manager is focused on policy and event management.

However, the following topics describe some management activities that you can perform using Security Manager:

Managing IPS Licenses

The following topics explain how to manage licenses for IPS devices:

Updating IPS License Files

You can use Security Manager to update the licenses for IPS devices. This procedure explains how to update the licenses manually by retrieving them from Cisco.com or from a license file on the Security Manager server. For information about setting up automatic license updates, see Automating IPS License File Updates , on page 3.

Before You Begin

If you use Cisco.com, you must first configure the IPS Update server to be Cisco.com, so that you can specify the username and password. You must use Cisco.com for licensing if you are using a device that requires it; for example, an IPS 4270 or an AIP SSM-40 in an ASA device requires a Cisco.com account. For information on configuring Cisco.com as the IPS Update server, see Configuring the IPS Update Server , on page 4.

If you use local licenses, you must download them directly to the Security Manager server file system. You cannot do this through Security Manager; you must log into Windows on the server to download the licenses.

Related Topics

• Redeploying IPS License Files , on page 2

Step 1 Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Step 2 Click the **IPS** tab (see IPS Tab, Licensing Page).

The table lists all IPS devices in the device inventory and displays the status of their licenses. The status can be valid, invalid, expired, no license, or trial license. The expiration date for the license is also shown. Click **Refresh License** to update the table with the latest license information from the devices (you can select one or more devices to limit the scope of the refresh).

To update licenses, do one of the following:

- To update devices with licenses obtained directly from Cisco.com—Select the devices you want to update and click **Update Selected via CCO**. A dialog box opens that lists the devices that can be updated from Cisco.com, which might not be all of the devices you selected. Review the list and click **OK**. The status of the update task is shown in the License Update Status Details dialog box (see License Update Status Details Dialog Box).

To successfully update the license using this method, you must have a Cisco.com support contract that includes the serial numbers of the selected devices.

Tip The Cisco software license server (SWIFT) that contains the licenses might block requests from the same server for more than 9 licenses within a three minute period. Thus, you should select fewer than 9 devices at a time when performing manual license updates.

- To update devices with licenses that you have copied to the Security Manager server—Click **Update from License File**. A dialog box opens where you can select the license files. Click **Browse** to select them from the Security Manager local file system. You can select more than one license file. When you have selected the desired files, click **OK** to have them applied to the devices.

Redeploying IPS License Files

If an attempt to apply an IPS license update to a device fails, you can redeploy the update. Redeployment works only if you have already attempted to apply an update and a license file is associated with the IPS device.

Related Topics

- Updating IPS License Files , on page 1
- Automating IPS License File Updates , on page 3

Step 1 Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Step 2 Click the **IPS** tab (see IPS Tab, Licensing Page).

Step 3 Select the devices to which you want to redeploy licenses and click **Redeploy Selected Licenses**. A dialog box opens listing devices whose licenses you are redeploying. Click **OK** to perform the update.

The status of the update task is shown in the License Update Status Details dialog box (see License Update Status Details Dialog Box).

Automating IPS License File Updates

Security Manager can automatically apply IPS license updates to your IPS devices on a regular schedule. To successfully configure automatic updates, you must have a Cisco.com support contract that includes the serial numbers of your IPS devices.

Tip Security Manager applies new licenses only if the downloaded license has an expiration date further into the future than the one replaced or if the license information is different.

Before You Begin

You must first configure the IPS Update server to be Cisco.com, so that you can specify the Cisco.com username and password. For information on configuring Cisco.com as the IPS Update server, see Configuring the IPS Update Server , on page 4.

Related Topics

- Updating IPS License Files , on page 1
- Redeploying IPS License Files , on page 2

Step 1 Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Step 2 Click the **IPS** tab (see IPS Tab, Licensing Page).

Step 3 Select **Download and apply licenses** and configure the following settings:

- **Days before the expiration date**—Select the number of days before a license expires that Security Manager should download an updated license. The default is 1 day.
- **Discover devices daily at**—Select the time of day when Security Manager should download licenses. At this time, Security Manager will check the license status on the devices, and contact Cisco.com for new licenses for devices that have no license, have expired licenses, or that have licenses that will expire within the number of days you selected.
- **Email License Update Results**—Select whether Security Manager should send e-mail notification of license update results. E-mails are sent with license expiration status and for license update job results. If you select this option, enter one or more e-mail addresses in the **Email Notification** field. Separate multiple addresses with commas.

For the e-mails to be sent, you must configure an SMTP server as described in Configuring an SMTP Server and Default Addresses for E-Mail Notifications.

Step 4 Click **Save** to save your changes.

Managing IPS Updates

You can use Security Manager to apply sensor and signature updates to your IPS devices and shared policies. Through Security Manager, you can download updates and either set up automatic updates or apply them manually.

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

Tip If you have problems applying patches, service packs, or signature updates, 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. For information on configuring NTP on the sensor, see Identifying an NTP Server.

The IPS packages included with Security Manager do not include the package files that are required for updating IPS devices. You must download IPS packages from Cisco.com or your local update server before you can apply any updates. The downloaded versions include all required package files and replace the partial files that are included in the Security Manager initial installation.

The following topics describe how to use Security Manager to manage IPS updates:

- Configuring the IPS Update Server , on page 4
- Checking for IPS Updates and Downloading Them , on page 5
- Automating IPS Updates , on page 6
- Manually Applying IPS Updates , on page 7

Configuring the IPS Update Server

To apply IPS sensor and signature updates, Security Manager must download the updates to the Security Manager server from an identified IPS Update server.

You can use Cisco.com as the IPS Update server. Using Cisco.com ensures that the latest updates are available to you at their earliest availability. However, if you cannot use Cisco.com for some reason, you can set up your own local IPS Update web server, manually download updates to it, and configure Security Manager to obtain the updates from your local server.

Tip If you are using a device that requires a Cisco.com login for updating licenses, such as an IPS 4270 or an AIP SSM-40 in an ASA device, you must configure the IPS Update server as Cisco.com. You cannot use a local server.

Related Topics

- Automating IPS Updates , on page 6
- Manually Applying IPS Updates , on page 7

Step 1 Select **Tools > Security Manager Administration** and select **IPS Updates** from the table of contents to open the IPS Updates page (see IPS Updates Page).

Step 2 In the Update Server area, click **Edit Settings** to open the Edit Update Server Settings dialog box (see Edit Update Server Settings Dialog Box).

Step 3 Enter the identifying information for your server. Based on the server type selected in the Update From field:

- Cisco.com—Enter a Cisco.com username and password. The user account you specify must have applied for eligibility to download strong encryption software. To verify the account has the appropriate permissions, go to Cisco.com and try to download an IPS update package. You will be prompted to accept the appropriate agreements if the account is not already qualified.
- Local server—Enter the IP address or DNS host name of your server, a username and password if you require a log in before allowing access, and the path to the folder that contains the files. For the path, do not enter the entire URL; enter only the path portion of the URL (for example, the path in http://servername/IPSpath is IPSpath). Also add IIS configuration settings:
  - Home Directory should have listing enabled.
  - Documents should have Default Content Page disabled.

Enter certificate information. Before you can download an IPS package, you must accept the Cisco.com certificate. You must accept the certificate from both the "Image Meta-data locator" site and the download site of the IPS packages to start downloading images successfully (see Edit Update Server Settings Dialog Box).

If your network requires a proxy server to get from the Security Manager server to the IPS Update server, select **Enable Proxy Server** and enter the information for the proxy server.

Click **OK** to save your changes.

Step 4 Click **Save** on the IPS Updates page. Your changes are not completely saved unless you click **Save**.

Step 5 Test the connectivity to the IPS Update server by clicking **Download Latest Updates**. A dialog box opens. Click **Start** to have Security Manager log into the update server, check for new updates, and download them. The dialog box displays the results of the operation.

If you are using Cisco.com and experience a download failure, double-check the user account to ensure it has the required permissions for downloading strong encryption software.

Checking for IPS Updates and Downloading Them

You can use Security Manager to check for IPS sensor and signature updates and download them to the Security Manager server, where you can apply them to your IPS devices and policies.

You can manually download IPS updates, automate IPS update downloads, or download them when you try to manually apply them to a device. The following procedure explains how to manually check for updates and download them. For information on configuring automatic downloads, see Automating IPS Updates , on page 6. For information on downloading updates while manually applying them to devices or policies, see Manually Applying IPS Updates , on page 7.

Before You Begin

You must configure the IPS Update server as described in Configuring the IPS Update Server , on page 4.

Related Topics

- Automating IPS Updates , on page 6
- Manually Applying IPS Updates , on page 7

Step 1 Select **Tools > Security Manager Administration** and select **IPS Updates** from the table of contents to open the IPS Updates page (see IPS Updates Page).

Step 2 Review the status information in the Update Status group, and do any of the following:

- Click **Check for Updates**. A dialog box opens to display the results of the operation. Click **Start** to have Security Manager log into the IPS Update server and check for updates.
- Click **Download Latest Updates**. A dialog box opens to display the results of the operation. Click **Start** to have Security Manager log into the IPS Update server, check for updates, and download them to the Security Manager server.

Tip If a Cisco.com download fails, ensure that the account you are using has applied for eligibility to download strong encryption software. For details, see the description of User Name in Edit Update Server Settings Dialog Box.

Automating IPS Updates

You can automatically apply sensor image and signature updates to compatible IPS devices to ensure that they are up to date. If desired, you can partially automate the updates to maintain the desired level of control over the process.

Tip If you later decide that you did not want to apply a signature update, you can revert to the previous update level by selecting the Signatures policy on the device, clicking the **View Update Level** button, and clicking **Revert**.

Tip If you do not manage IPS devices, consider taking the following performance tuning step. In *$NMSROOT* \MDC\ips\etc\sensorupdate.properties, change the value of packageMonitorInterval from its initial default value of 30,000 milliseconds to a less-frequent value of 600,000 milliseconds. Taking this step will improve performance somewhat. [*$NMSROOT* is the full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).]

Before You Begin

You must configure the IPS Update server as described in Configuring the IPS Update Server , on page 4.

Related Topics

- Checking for IPS Updates and Downloading Them , on page 5
- Manually Applying IPS Updates , on page 7

- Understanding IPS Network Sensing
- Deploying Configurations in Non-Workflow Mode
- Deploying Configurations in Workflow Mode

Step 1 Select **Tools > Security Manager Administration** and select **IPS Updates** from the table of contents to open the IPS Updates page (see IPS Updates Page).

Step 2 In the Auto Update Settings group in the lower portion of the page, select an auto update mode to establish the extent of automation. Choices include:

- Download, Apply, and Deploy Updates—Security Manager checks for updates according to your schedule, downloads them to the Security Manager server, applies them to the selected devices and policies, and starts a deployment job to update the affected devices. This choice ensures that your devices are running the latest updates with minimal effort for your operations staff.
- Disable Auto Update—Security Manager does not perform any automatic actions for IPS updates.
- Check for Updates—Security Manager checks for updates according to your schedule and updates the information in the Update Status group. No devices or policies are updated.
- Download Updates—Security Manager checks for updates according to your schedule and downloads any new updates to the Security Manager server.
- Download and Apply Updates—Security Manager checks for updates according to your schedule, downloads them, and applies them to the selected devices and policies. You must separately create a deployment job to deploy the changes to the affected devices.

Step 3 Click **Edit Update Schedule** to open a dialog box where you can specify the schedule for the operation. Select the starting date, enter the starting time in 24-hour format (hh:mm), and select whether the schedule should be by the hour, day, week, month, or a one-time event. Click **OK** to save the schedule.

Step 4 (Optional) Enter an e-mail address in the Notify Email field. Security Manager will notify this user when a package is available for download or has been downloaded, applied, or deployed. You can enter more than one address by separating the addresses with commas.

Step 5 Select the devices and shared policies you want to automatically update in the Apply Update To selector. Use the Type field to toggle between local policies (for devices) and shared policies.

To select a device or policy, click it in the selector and click the **Edit Row** button (the pencil icon below the selector). This action opens the Edit Auto Update Settings dialog box. Select the types of updates you want to apply: minor sensor updates and service packs or service packs only, and the signature update level. Click **OK** to save your changes. The devices to which the policy apply are added to the Devices to be Auto Updated list. A message will indicate if you need to submit your changes for the change to take effect.

Step 6 Click **Save**.

Manually Applying IPS Updates

You can manually apply image and signature updates to compatible IPS devices using the Apply IPS Update wizard. Use this procedure with policies and devices that you did not configure for automatic updates (as described in Automating IPS Updates , on page 6).

When applying signature updates, the wizard displays those signatures in the update that are not configured on the target IPS devices. You can configure the new signatures before they are applied.

When applying image and signature updates, only those devices to which the updates can be applied are available for selection. Inapplicable devices are grayed out. If you hover the mouse pointer over a grayed out device, a tooltip displays the reason for graying out the device. A device can be grayed out even if a signature update applies to it but if the required engine upgrade or generic packages are not available. Following are some of the instances when devices might be grayed out and the corresponding tooltip labels:

- If the version of the selected signature or sensor package is lower than the version of the target IPS device, Security Manager grays out the device and a mouse-over tooltip displays the message "Selected package is inapplicable".
- 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". This is because SNMPv3 is not supported in IPS version 7.3.1.
- If you try to use Security Manager to perform a signature update that does not contain one or more threat profiles applied to the device, Security Manager grays out the device and a mouse-over tooltip displays the message "Currently applied threat profile is not applicable to this signature version". It does not allow the signature update to be successfully applied. You must remove the existing threat profile and then proceed with the signature update.

Tip If you later decide that you did not want to apply a signature update, you can revert to the previous update level by selecting the Signatures policy on the device, clicking the **View Update Level** button, and clicking **Revert**.

Before You Begin

Configure the IPS Update server as described in Configuring the IPS Update Server , on page 4.

Related Topics

- Checking for IPS Updates and Downloading Them , on page 5
- Selecting a Signature Category for Cisco IOS IPS

Note This note describes a difference between the update packages for IPS 7.1.3 and those used for earlier versions. When you open the Apply IPS Update wizard (Tools > Apply IPS Update), the first page of the wizard lists the sensor and signature update packages that are available. Beginning with IPS 7.1.3, a single update package is used for all supported platforms, such as IPS-4270 and ASA-SSE-AIP-85; example: IPS-CSM-K9-7.1.3.zip. Prior to IPS 7.1.3, a separate package was used for each supported platform; example: IPS-CS-MGR-SSC_5-K9-6.2-4-E4.zip.

Step 1 Select **Tools > Apply IPS Update** to open the Apply IPS Update wizard.

Step 2 On the first page of the wizard, select the update that you want to apply. This page lists the sensor and signature updates that are available. Do the following on this page:

- To update the list of packages, click **Download Latest Updates**. Security Manager logs into the IPS Update server and downloads the updates that have become available since the last download. This works only if you have configured an update server as described in Configuring the IPS Update Server , on page 4. You can also update the list of packages by doing the following:
  - Configure automatic downloads on the IPS Updates page (select **Tools > Security Manager Administration > IPS Updates**). For more information, see IPS Updates Page.
  - Manually download the updates to the CSCOpx\MDC\ips\updates folder in the product installation folder (typically Program Files) on the Security Manager server.

You can also check for updates without downloading them by clicking **Check for Updates**. The Update Status information is the same as described in IPS Updates Page.

- Select the signature or sensor update you want to apply to your IPS devices in the Updates Downloaded table. Use the **Type** field to toggle between the types of updates (you can select only one update to apply):
  - **Sensor Updates**—Displays the filename, the major, minor, service pack, and patch versions, as well as the supported engine release. You must apply all major sensor updates, however, minor updates are cumulative.
  - **Signature Updates**—Displays the filename, the signature number, and the supported engine release. Signature updates are cumulative; however, applying them as separate packages allows you to separate your work into more manageable units if you intend to tune the updates to match the specific needs of your network.

Note The engine package is not listed on the update page, but Security Manager implicitly pushes the engine package automatically in the case of a signature update that requires a higher engine version. (This occurs only when updating a device with the particular version that the engine package requires.)

Click **Next** to continue.

Step 3 On the second page of the wizard, select the local signature policies (representing devices not assigned to any shared signature policy) and shared signature policies you want to update from the Apply Updates To list. Use the **Type** field to toggle between the types of policies. You can select any combination of local and shared policies. When you select a policy, the devices that use the policy are selected for update.

To select all applicable devices or shared policies, click **Select All**. To erase your selection and start over, click **Deselect All**. These buttons apply only to the displayed list.

IPS devices to which the update does not apply are grayed out in the Apply Updates To list, and you cannot select them. When you select a device that can be updated, it is listed in the Devices Assigned to Selected Policies list; these are the only devices that will be updated. If you select a shared policy, all devices that are using the policy appear in the selected policies list, but the devices to which the update does not apply are grayed out.

Tip The engine release controls which devices you can select for sensor updates; you can apply the update only to devices that use the same engine version, regardless of the release version. For example, if your device is running 6.0(5) E3, you can update to 6.1(1) E3 but not to 6.1(1) E2. You also cannot apply a 6.1(1) E3 update to a device running 6.1(1) E2. If you want to update the engine version, select a signature update with the higher engine version, and Security Manager will update the engine level automatically while updating the signatures. For example, if the device has the 6.1(1) E2 version and needs to have the E3 engine package applied, choose the signature package that requires the E3 engine and apply it to the device; doing so applies the engine package automatically to the device while updating the signatures. Thus, if the device you want to update is grayed out, click **Back** and change your update selection.

If you are applying a signature update, and you want to edit the signatures before applying them, click **Next** to continue. Otherwise, click **Finish** to apply your update to the policies.

Step 4 (Optional) On the third page of the wizard, modify the signatures as desired.

The signatures list displays the new and modified signatures between the signature level of the selected update and the lowest signature level among the selected devices. If the selected devices include both IPS sensors and Cisco IOS IPS devices, the signatures for these devices appear on separate tabs.

Click the link in the ID number to read the description for the signature on Cisco.com. The Status column indicates whether the signature is new or modified (see the visual description of the icons on the wizard page).

To edit a signature, select it in the table and click the Edit button below the table (the pencil icon). For help in understanding the signature, click **Help** in the dialog box that the Edit button opens.

For details on available signature information, see Signatures Page. In the Signature Summary Table, you can also add custom signatures and delete signatures, but you cannot do that on this page of the Apply IPS Update Wizard.

Click **Finish** to apply your update to the policies and to save your edits.

Step 5 Submit your changes and deploy them to the devices. For information on creating deployment jobs, see these topics:

- Deploying Configurations in Non-Workflow Mode
- Deploying Configurations in Workflow Mode

Managing IPS Certificates

When you configure Security Manager to use SSL (HTTPS) to communicate with your IPS devices, the certificate configured on the device must match the certificate stored in Security Manager's certificate store. Mismatched certificates will result in communication failures during policy discovery or deployment.

IPS devices use self-signed certificates that have a fixed validity period of about 2 years. When the certificate expires, you need to regenerate the certificate and update the certificate store with the new certificate.

Security Manager includes a utility that you can use to synchronize the certificate store with the certificate defined on the device, to regenerate expired certificates, and to view the status of certificates (including expiration dates) on the IPS devices that you manage.

Tip If you are using HTTP for communication with the IPS devices, certificates are not used and you cannot manage them. IPS device communication settings are configured in the Security Manager Administration Device Communication page (see Device Communication Page).

The following procedure explains how to manage your IPS certificates with Security Manager.

Related Topics

- Table Columns and Column Heading Features
- Filtering Tables
- Manually Adding SSL Certificates for Devices that Use HTTPS Communications
- Security Certificate Rejected When Discovering Device
- Invalid Certificate Error During Device Discovery

Step 1 Select **Manage > IPS > IPS Certificates** to open the IPS Certificates dialog box.

Tip The list shown in this dialog box is not automatically refreshed. Click **Refresh** whenever you open the dialog box to ensure that you are looking at the most current certificate expiration information.

The dialog box lists all IPS sensors that are in the inventory according to their Security Manager display name. Not all columns are displayed (right-click any cell heading to select additional columns). The main columns of interest are the following:

- **Certificate Mismatch?**—Whether the certificate defined on the device is the same as that in Security Manager. This field is blank if the certificate is unavailable or non-retrievable; otherwise, it can have these values:
  - **No**—The device and Security Manager have the same certificate. No action is required.
  - **Yes**—The device and Security Manager have different certificates. If the certificate has not expired, select the device and click **Sync Certificates** to replace the certificate in the Security Manager certificate store with the certificate from the device.
- **Valid Until on Device, Valid From on Device**—These two separate columns show the date range within which the certificate is valid. The certificate expires after the Valid Until date is reached. Consider regenerating the certificate as this date approaches.
- **Certificate Status on Device**—Shows the current status of the certificate as it exists on the device:
  - **Valid Certificate**—The certificate is good and within the validity date range.
  - **Expired Certificate**—The certificate has passed its Valid Until date and is now expired. Select the device and click **Regenerate Certificate** to create a new valid certificate on the device and to have the certificate loaded into the Security Manager certificate store.
  - **Certificate Not Yet Valid**—The certificate has not yet reached its Valid From date and cannot be used yet. This might indicate a mismatch between the time settings on the device and on the Security Manager server. Ensure that the time settings are the same (consider using an NTP server). Consider regenerating the certificate.
  - **Unavailable – Refresh to get Cert Info**—The certificate is not currently in the Security Manager certificate store. Click **Refresh** to have Security Manager retrieve the certificate from the device and load it into the certificate store.
  - **Nonretrievable – Cert Info not available**—Security Manager was not able to log into the device and retrieve the certificate, or you are using HTTP for communications. Select the device and click **Refresh**.

If refresh does not resolve the problem, ensure that the device is operating normally (that it is not down), and then check the device properties to ensure that correct credentials are configured for access (see Viewing or Changing Device Properties). If credentials are not the problem, also check the Allowed Hosts policy configured on the device and ensure that the Security Manager server is included as an allowed host (see Identifying Allowed Hosts). You can also log into Windows on the Security Manager server and use ping to see if there is a route between the server and the IPS device.

- **Thumbprint on CSM, Thumbprint on Device**—These separate columns show the thumbprint for the certificate in the certificate store and on the device.

Step 2 Use any of the following buttons to perform the indicated actions. Except where indicated, if you do not select one or more devices before clicking the button, the action is performed on all listed devices, which can be time-consuming if there are a lot of IPS devices. You are warned before an operation is performed on all devices and given the option to stop it.

- **Sync Certificate**—Synchronize the certificate information in the Security Manager certificate store with the certificate on the device. The device certificate replaces the one in the certificate store.
- **Regenerate Certificate**—Generate a new certificate on the device and then load the new certificate into the certificate store.
- **Refresh**—Refresh the status information by having Security Manager contact the devices and retrieve certificate information, such as validity dates, and compare the certificate with the one in the certificate store. This action updates the Certificate Status on Device column and also determines whether there is a certificate mismatch.
- **Export**—Exports the entire certificates table to a comma-separated values (CSV) file. You cannot export less than the entire table. You are prompted for a file name and folder on the Security Manager server.

Rebooting IPS Sensors

You can reboot an IPS sensor from Security Manager.

To reboot the sensor, select it in Device view, right-click and select **Reboot Device**. You are asked to confirm that you want to reboot.

Security Manager does not provide status information on the reboot process.