



CHAPTER 20

Managing the Security Manager Server

The following topics describe some system management tasks related to the general operation of the Security Manager product:

- [Overview of Security Manager Server Management and Administration, page 20-1](#)
- [Configuring Administrative Settings, page 20-2](#)
- [Managing Licenses, page 20-3](#)
- [Managing IPS Updates, page 20-7](#)
- [Working with Audit Reports, page 20-11](#)
- [Taking Over Another User's Work, page 20-13](#)
- [Backing up and Restoring the Security Manager Database, page 20-14](#)
- [Creating a Diagnostics File for the Cisco Technical Assistance Center, page 20-15](#)

Overview of Security Manager Server Management and Administration

As a software application, Cisco Security Manager runs on the framework provided by the CiscoWorks Common Services application. Many of the fundamental server control functions are provided by Common Services. For example, if you want to create a multiple-server setup for Security Manager, you must create that setup in Common Services. Common Services also provides the tools for creating and managing local user accounts, for backing up and restoring the database, for generating various reports on system functions, and for many other basic functions.

To access the Common Services application, do any of the following:

- If you currently have the Security Manager client open, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. You can click any button and then navigate to any desired page in Common Services.
- Using your web browser, link to the Security Manager server using the URL `https://servername`, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration**, or the **CiscoWorks** link, to open Common Services.

To learn more about the things you can do with Common Services, browse the Common Services online help.

Configuring Administrative Settings

Security Manager has default settings for many system functions that you can change if they do not fit the needs of your organization. To view and change these settings, select **Tools > Security Manager Administration**. You can then select items from the table of contents on the left of the window to view the default settings related to that item.

On most pages, when you change a setting, you must click **Save** to save your changes. If you make a mistake, you can click **Reset** to return the values to the previously saved values. You can also click **Restore Defaults** to return the settings to the Security Manager defaults.

Besides the pages that contain system defaults, the Security Manager Administration window includes items that relate to system administration activities, such as taking over another user's work or obtaining access to pages in Common Services to perform server security tasks.

The following topics describe the settings and actions available on each of the pages available in the Security Manager Administration window:

- [AutoLink Settings Page, page A-2](#)
- [Configuration Archive Page, page A-2](#)
- [CS-MARS Page, page A-3](#)
- [Customize Desktop Page, page A-5](#)
- [Debug Options Page, page A-6](#)
- [Deployment Page, page A-7](#)
- [Device Communication Page, page A-11](#)
- [Device Groups Page, page A-14](#)
- [Device OS Management Page, page A-15](#)
- [Discovery Page, page A-16](#)
- [IPS Updates Page, page A-17](#)
- [Licensing Page, page A-28](#)
- [Logs Page, page A-32](#)
- [Policy Management Page, page A-33](#)
- [Policy Objects Page, page A-34](#)
- [Rule Expiration Page, page A-35](#)
- [Server Security Page, page A-36](#)
- [Status Page, page A-37](#)
- [Take Over User Session Page, page A-40](#)
- [Token Management Page, page A-40](#)
- [VPN Policy Defaults Page, page A-41](#)
- [Workflow Page, page A-44](#)

Managing Licenses

The following topics explain how to install licenses for the Security Manager application and how to manage licenses for IPS devices:

- [Installing Security Manager License Files, page 20-3](#)
- [Updating IPS License Files, page 20-4](#)
- [Redeploying IPS License Files, page 20-5](#)
- [Automating IPS License File Updates, page 20-6](#)
- [Getting Help with Licensing, page 20-6](#)

Installing Security Manager License Files

The terms of your Security Manager software license determine many things, including the features that are available to you and the number of devices that you can manage. For licensing purposes, the device count includes any physical device, security context, virtual sensor, or Catalyst security services module that uses an IP address. Failover pairs count as one device. For PIX Firewalls, FWSM, and ASA devices that are configured in multiple-context mode (so that they host more than one security context), only the security contexts are counted as devices; the hosting device is not counted as a separate device.

When you upgrade from an earlier release, Security Manager does not prompt you for a license; instead, it retains your license and continues to enforce its terms. If you upgrade during a free evaluation, the remaining time in your evaluation period does not change.

Two license types, Standard and Professional, are available, in addition to a free 90-day evaluation period that is restricted to 50 devices. For complete information on the types of licenses available and the various supported upgrade paths, as well as information about the Cisco Software Application Support service agreement contracts that you can purchase, see the product bulletin for this version of Security Manager at http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html.

License limits are imposed when you exceed the allotted time (in the case of the evaluation license), or the number of devices that your license allows you to manage. The evaluation license provides the same privileges as the Professional Edition license. It is important that you register Security Manager as soon as you can within the first 90 days, and for the number of devices that you need, to ensure uninterrupted use of the product. Each time you start the application you are reminded of how many days remain on your evaluation license, and you are prompted to upgrade during the evaluation period. At the end of the evaluation period, you are prevented from logging in until you upgrade your license.

**Tip**

The number of devices includes all discovered security contexts and virtual sensors, even if you have not submitted the activity that discovered them and they do not currently appear in the device selector. If it appears there are fewer devices in the inventory than your license allows, but you are getting device count error messages, submit all activities to determine the number of discovered devices. Delete those that you do not want to manage.

Before You Begin

- Obtain the base license and any additional licenses you require. You must have a Cisco.com user ID, and you must register your copy of the software on Cisco.com. When registering, you must provide the Product Authorization Key (PAK) that is attached to the Software License Claim Certificate inside the shipped software package.

- If you are a registered Cisco.com user, go to <http://www.cisco.com/go/license>.
- If you are not a registered Cisco.com user, go to <http://tools.cisco.com/RPF/register/register.do>.

After registration, the base software license is sent to the e-mail address that you provided during registration. In addition to receiving a PAK and license for Security Manager, you might receive one additional PAK for each incremental device count pack you purchased.

Copy the license files to a folder on the Security Manager server. You must store your license files on a disk that is local to your Security Manager server; you cannot use a drive that is mapped to the server. Windows imposes this limitation, which serves to improve Security Manager performance and security.

**Tip**

Do not place the license file in the etc/licenses/CSM folder in the product's installation folder, or you will encounter an error when you try to add the license. Place the file in a folder outside the product folders.

- Common Services does not require a license file.
- Auto Update Server does not require a license file.

Procedure

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

Step 2 Click **CSM** if the tab is not active. For a description of the fields on this tab, see [CSM Tab, Licensing Page, page A-29](#).

Step 3 Click **Install a License** to open the Install a License dialog box.

The Install a License dialog box includes links to Cisco.com for obtaining licenses if you have not already done so. If you already have copied the licenses to the Security Manager server, click **Browse** to select a license file, and then click **OK** on the Install a License dialog box to install the license.

Repeat the process until you have installed all of your licenses.

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, page 20-6](#).

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, page 20-7](#).

Related Topics

- [Redeploying IPS License Files, page 20-5](#)

Procedure

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, page A-29](#)).

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.

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, page A-31](#)).



Tip 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.

- 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, page 20-4](#)
- [Automating IPS License File Updates, page 20-6](#)

Procedure

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, page A-29](#)).

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, page A-31](#)).

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.

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, page 20-7](#).

Related Topics

- [Updating IPS License Files, page 20-4](#)
- [Redeploying IPS License Files, page 20-5](#)

Procedure

-
- 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, page A-29](#)).
- Step 3** Select **Download and Apply Licenses Automatically**.
- Step 4** In the **Check** field, select how often Security Manager should check Cisco.com for new licenses:
- Daily—Once a day at midnight
 - Weekly—Once a week at midnight on Sunday
 - Monthly—Once a month at midnight on the first day of the month.
-

Getting Help with Licensing

If you have trouble using the registration website, contact the Licensing Department in the Cisco Technical Assistance Center (TAC):

- Phone: +1 (800) 553-2447
- E-Mail: licensing@cisco.com
- <http://www.cisco.com/tac>

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

- [Configuring the IPS Update Server, page 20-7](#)
- [Checking for IPS Updates and Downloading Them, page 20-8](#)
- [Automating IPS Updates, page 20-9](#)
- [Manually Applying IPS Updates, page 20-10](#)

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, page 20-9](#)
- [Manually Applying IPS Updates, page 20-10](#)

Procedure

- 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, page A-17](#)).
- 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, page A-21](#)).
- 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`).

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, page 20-9](#). For information on downloading updates while manually applying them to devices or policies, see [Manually Applying IPS Updates, page 20-10](#).

Before You Begin

You must configure the IPS Update server as described in [Configuring the IPS Update Server, page 20-7](#).

Related Topics

- [Automating IPS Updates, page 20-9](#)
- [Manually Applying IPS Updates, page 20-10](#)
- [Chapter 13, “Managing IPS Services”](#)

Procedure

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, page A-17](#)).

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](#), page A-21.

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.

Before You Begin

You must configure the IPS Update server as described in [Configuring the IPS Update Server](#), page 20-7.

Related Topics

- [Checking for IPS Updates and Downloading Them](#), page 20-8
- [Manually Applying IPS Updates](#), page 20-10
- [Chapter 13, “Managing IPS Services”](#)
- [Understanding Network Sensing](#), page 13-1
- [Deploying Configurations in Non-Workflow Mode](#), page 18-17
- [Deploying Configurations in Workflow Mode](#), page 18-19

Procedure

-
- 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](#), page A-17).
- 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, page 20-9](#)).

Before You Begin

You must configure the IPS Update server as described in [Configuring the IPS Update Server, page 20-7](#).

Related Topics

- [Automating IPS Updates, page 20-9](#)
- [IPS Updates Page, page A-17](#)
- [Chapter 13, “Managing IPS Services”](#)

Procedure

- Step 1** Click **Tools > Apply IPS Update** to open the Apply IPS Update wizard (see [Apply IPS Update Wizard, page A-23](#)).
- Step 2** On the first page of the wizard, select the update that you want to apply (see [Step 1: Select Update To Apply Page, page A-24](#)). 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.
 - Select the signature or sensor update you want to apply in the table. Use the Type field to toggle between the types of updates. You can select only one update to apply.



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 devices (local policies) and shared policies you want to update (see [Step 2: Select Policies Update Will Be Applied To Page, page A-26](#)). Use the Type field to toggle between the types of policies. You can select any combination of local and shared policies.

The devices to which the updates apply appear in the Devices Assigned to Selected Policies list. A greyed-out device name indicates the update does not apply to the device.



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.

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 (see [Step 3: Edit Signatures Page, page A-27](#)). To modify a signature, select it and click the Edit button below the table (the pencil icon). For more information about editing the signature, click **Help** in the dialog box that the Edit button opens.

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

Step 5 Deploy your changes to the devices. For information on creating deployment jobs, see these topics:

- [Deploying Configurations in Non-Workflow Mode, page 18-17](#)
- [Deploying Configurations in Workflow Mode, page 18-19](#)

Working with Audit Reports

When state changes occur in Security Manager, an audit entry is created in the audit log, which you can view by selecting **Tools > Audit Report**. The following topics provide more detailed information about audit reports:

- [Understanding Audit Reports, page 20-11](#)
- [Generating the Audit Report, page 20-12](#)
- [Purging Audit Log Entries, page 20-13](#)

Understanding Audit Reports

When state changes occur in Security Manager, an audit entry is created in the audit log, which you can view by selecting **Tools > Audit Report**.

The state changes that generate an event and create an audit entry are:

- Changes to the runtime environment:

- System changes, such as login attempts (successful or failed), logout, and scheduled backups.
- Authorization issues, such as failed attempts and security breaches.
- Map changes, such as saving, deleting, and changing background map views.
- Administrative changes, such as changing workflow modes.
- Changes to the state of Security Manager objects:
 - Activity changes, such as creating, editing, submitting, or approving an activity.
 - Deployment changes, such as creating, editing, or submitting a deployment job.
- Changes to the state of managed devices:
 - Object changes, such as changes to policy objects.
 - Inventory changes, such as adding, deleting, or modifying devices in the inventory.
 - Policy changes, such as creating, restoring, modifying, or deleting policies.
 - VPN changes, such as creating, modifying, or deleting a VPN.

When viewing the audit report, you can view subsets of entries by specifying search criteria to select only the desired records.

Related Topics

- [Generating the Audit Report, page 20-12](#)
- [Purging Audit Log Entries, page 20-13](#)

Generating the Audit Report

You can view the audit log to analyze the events that have occurred in the Security Manager System. This information can help you track changes that users have made to devices or to identify other system events of interest. The Audit Report window provides extensive search criteria to help you view the specific audit log entries that interest you.



Tip

You can also view the audit logs through CiscoWorks Common Services. From the Common Services Server Administration page, select **Server > Reports**, and select **Audit Log** from the table of contents. Click **Generate Report** and you are presented with a list of logs, one for each day. Click the link for the desired log to open it. These logs are stored in the Program Files/CSCOPx/MDC/Logs/audit/ directory. For information about logging into Common Services, see [Logging In to the Cisco Security Management Suite Server, page 1-8](#).

Related Topics

- [Understanding Audit Reports, page 20-11](#)

Procedure

- Step 1** Select **Tools > Audit Report** to open the Audit Report window.
- Step 2** To reduce the report to a specific set of records that relate to an area of interest, enter the appropriate search criteria in the left pane and click **Search**. For detailed information about the search fields, see [Audit Report Window, page E-9](#).

The following examples describe sample search criteria:

- To find out when the device `router1` was removed from Security Manager management—Select **Devices > Delete** from the **Search by action** selector. In the **Search by all or part of the object name** field, enter the display name of the device (`router1`).
- To find out if a failed login attempt occurred in the system—Select **System > Authorization > Login > Failed** from the **Search by action** selector.

Step 3 To view the contents of an entry in the report, double click the entry. This action opens a dialog box where you can read the message related to the entry. You can scroll through the report in this dialog box by using the up and down arrow buttons.

Purging Audit Log Entries

Security Manager automatically prunes the audit logs based on the age of the log entries. You do not need to actively manage the size of the log. However, you can change the defaults to increase or decrease the maximum size of the log and thus manage the overall size of the database.

To change the default settings for audit logs, select **Tools > Security Manager Administration** and select **Logs** from the table of contents (see [Logs Page, page A-32](#)). The size of the log is controlled by the maximum number of days an entry can be, and the overall maximum number of entries that can be in the log. These settings work together, and entries are pruned on a periodic basis to keep the log to the maximum number of entries with none that are older than the maximum number of days. If you reduce the maximum size of the log, click **Purge Now** to delete the excess entries before the regular pruning cycle.

You can also control the size of the log by changing the severity level of events that are captured in the log. For example, if you capture only Severe events, the log will probably remain small. However, reducing the level of information might reduce the value of the log.

Related Topics

- [Understanding Audit Reports, page 20-11](#)
- [Generating the Audit Report, page 20-12](#)
- [Audit Report Window, page E-9](#)

Taking Over Another User's Work

A user with administrative privileges can take over the work of another user in non-Workflow mode. Taking over another user's work is useful when a user is working on devices and policies, causing the devices and policies to be locked, and another user needs access to the same devices and policies.

Procedure

-
- Step 1** Select **Tools > Security Manager Administration** and select **Take Over User Session** from the table of contents to open the Take Over User Session page (see [Take Over User Session Page, page A-40](#)).
- Step 2** Select the user session you want to take over.
- Step 3** Click **Take over session**. The changes made by the selected user are transferred to you. Any changes that have not already been committed are discarded.

If the selected user is logged in at the time changes are taken over, the user receives a warning message, loses the changes in progress, and then is logged out.

Backing up and Restoring the Security Manager Database

Security Manager uses CiscoWorks Common Services facilities to back up and restore its database. In the Security Manager client, select **Tools > Backup** to open the CiscoWorks Common Services Backup page for creating a backup schedule. You should regularly back up the database so that you can recover it if necessary.

To learn about how to back up and restore the database, click the Help link in the upper right corner of the CiscoWorks Common Services Backup page. You must use offline commands to restore the database, so you might want to print the restore procedure. While backing up and restoring data, both Common Services and Security Manager processes will be shut down and restarted.



Tip

Because Security Manager can take several minutes to fully restart, users might be able to start their client before the restart is complete. If this happens, they might see the message “err loading page” in device policy windows.

We strongly recommend you take a backup of your current system before restoring an older backup.

You cannot restore a backup from an earlier version of Security Manager if that backup contains any pending data, which is data that has not been committed to the database. Before upgrading to a new version of Cisco Security Manager, we recommend that you commit or discard all uncommitted changes and then create a backup of your database. You can use the following instructions to help with committing or discarding pending data:

In non-Workflow mode:

- To commit changes, select **File > Submit**.
- To discard uncommitted changes, select **File > Discard**.

If there are multiple users with pending data, the changes for those users must also be committed or discarded. If you need to commit or discard changes for another user, you can take over that user’s session. To take over a session, select **Tools > Security Manager Administration > Take Over User Session**, select the session, and click **Take Over Session**.

In Workflow mode:

- To commit and approve changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve**. If you are using an activity approver, click **Submit** and have the approver approve the activity.
- To discard uncommitted changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

Creating a Diagnostics File for the Cisco Technical Assistance Center

Cisco Technical Assistance Center (TAC) personnel might ask you to submit system configuration information when you submit a problem report. This information assists them with diagnosing the problem. You do not need to submit a diagnostics file unless asked to do so.

Before you create the diagnostic file, perform the actions that lead to the problem you are reporting. If necessary, you can control the level of detail in the diagnostic information by changing the settings on the Debug Options page (select **Tools > Security Manager Administration > Debug Options**). For more information, see [Debug Options Page, page A-6](#).

To create the diagnostics file:

- Using the Security Manager client—Select **Tools > Security Manager Diagnostics**. A dialog box is opened. Click **OK** to start the file generation. The dialog box displays the progress. When the file is generated, click **Close**.
- Using the Windows command line on the Security Manager server—Open a Windows command line window on the server (for example, select **Start > Run** and enter **command**). Run the C:\Program Files\CSCOpX\MDC\bin\CSMDiagnostics program. If you want to, you can specify an alternate folder where the diagnostic file will be created (for example, **CSMDiagnostics C:\Temp**).

**Tip**

When creating the diagnostics file from the command line, you must allow the command to complete before closing the window or subsequent attempts to run the CSMDiagnostics command will not work properly. If you mistakenly close the window, delete the C:\Program Files\CSCOpX\MDC\etc\mdcsupporttemp folder before attempting to use the command again.

Unless you specify an alternate folder, the CSMDiagnostics.zip file is placed in the `<installation_location>/CSCOpX/MDC/etc` folder, where `<installation_location>` is the drive and directory in which you installed CiscoWorks Common Services (for example, c:\Program Files). You should move or rename the diagnostics file after you create it because the file is overwritten each time you generate it.

The CSMDiagnostics.zip file contains:

- Configuration files.
- Apache configuration and log files.
- Tomcat configuration and log files.
- Installation, audit, and operation log files.
- The CiscoWorks Common Services Registry subtree ([HKEY_LOCAL_MACHINE][SOFTWARE][Cisco][MDC]).
- Windows System Event and Application Event log files.
- Host environment information (operating system version and installed service packs, amount of RAM, disk space on all volumes, computer name, and virtual memory size).

