



# CHAPTER 20

## Using Tools

---

The Tools menu provides access to these device and network management features:

- **Device Properties**—Provides general information about the device, credentials, the group the device is assigned to, and policy overrides. For more information, see [Understanding Device Properties, page 5-51](#).
- **Policy Object Manager**—Allows you to view all available objects grouped according to object type, access all object dialog boxes to create, copy, edit, and delete objects, and generate usage reports, which describe how selected objects are being used by other Security Manager objects and policies. For information see “[Policy Object Manager User Interface Reference](#)” section on page F-1.
- **Site-To-Site VPN Manager**—Enables you to configure site-to-site VPNs. For information, see [Site-to-Site VPN Manager Window, page G-2](#).
- **Deployment Manager**—Enables you to deploy configurations and manage deployment jobs. For information, see [Appendix O, “Deployment User Interface Reference.”](#)
- **Activity Manager**—Allows you to create and manage activities. For information, see [Activity Manager Window, page E-1](#).
- **Policy Discovery Status**—Allows you to see the status of policy discovery and device import on the Policy Discovery Status page. For more information, see [Understanding Policy Discovery Status, page 20-3](#).
- **Show Containment**—Displays information about composite devices. For information, see [Understanding Show Containment, page 20-5](#).

- **Inventory Status**—Allows you to view and export device summary information for all devices. For information, see [Understanding Inventory Status, page 20-6](#).
- **Catalyst Summary Information**—Embedded in Security Manager, enables you to set up, configure, and monitor devices in the Cisco Catalyst 6500 and 7600 families. For information, see [Chapter 16, “Managing Catalyst Devices.”](#)
- **Device Manager**—Allows you to start device managers for all supported devices, such as PIX security appliances, Firewall Services Modules (FWSM), IPS sensors, IOS routers, and Adaptive Security Appliance (ASA) devices. Device managers provide several monitoring and diagnostic features that enable you to get information regarding the services running on the device and a snapshot of the overall health of the system. For more information, see [Device Managers, page 21-2](#).
- **IPS Event Viewer**—Offers a monitoring solution for small-scale IPS deployments. Monitoring individual IPS devices, IEV is easy to set up and lets you view and manage alerts for up to five sensors. For information, see [IPS Event Viewer, page 21-31](#).
- **Apply IPS Update**—The Apply IPS Updates wizard allows you to manually apply image and signature updates to compatible IPS devices. For information, see [Apply IPS Update, page Q-18](#).
- **Preview Configuration**—Displays the proposed changes, last deployed configuration, or current running configuration for specific devices. For information, see [Preview Config Dialog Box, page O-8](#).
- **Device OS Management**—Provides access to Resource Manager Essentials (RME) Software Image Manager (SWIM) and Inventory Reporting, according to access settings in the Security Manager administration pages. For more details see [Working With Device OS Management, page 20-6](#).
- **Audit Report**—Allows you to generate audit report data according to parameters set in the audit report page. For information, see [Understanding Audit Reports, page 20-7](#).
- **Change Reports (Activity Report)**—Allows you to generate a table of changes to devices, shared policies, and building blocks within a given activity (Workflow Mode) or configuration session (nonWorkflow Mode). For information, see [Understanding Audit Reports, page 20-7](#).

- Configuration Archive—Stores archived device configuration versions and allows you to view, compare and roll back from one configuration to another. For information, see [Using the Configuration Archive Tool, page 20-11](#).
- Backup—Allows backing up of Security Manager database using Common Services. For information, see [Backup and Restore, page 20-25](#).
- Security Manager Diagnostics—Describes how to gather troubleshooting information and contact the Technical Assistance Center (TAC). For information, see [Security Manager Diagnostics, page 20-26](#).
- Security Manager Administration—Details administrative settings, recommends which settings to define first, and explains user permissions and access modalities. For information, see [Performing Administrative Tasks, page 2-1](#).

## Understanding Policy Discovery Status

When you initiate policy discovery, a task is created. For each initiation, only one task is created regardless of the number of devices in the discovery.

You can see the status of policy discovery and device import on the Policy Discovery Status page. The Policy Discovery Status page contains three panes:

- Tasks pane—Provides status information for the overall task.
- Discovery Details or Import Details pane—Depending on the type of task, this pane is called either Discovery Details or Import Details. For each task you select in the Tasks pane, you will see corresponding information in the Discovery Details or Import Details pane.
  - The Discovery Details pane displays details about the policy discovery, such as the list of devices in the selected task, the status of the discovery (completed or failed), and the discovery method used (discovered from live device or discovered from file).
  - The Import Details pane displays details about the device import, such as the list of devices involved in the selected task, the task type for each device (import only or import and discover), and the status of device import (device added or device add failed).

- Messages pane—Contains three elements: Message Summary, Description, and Action. Displays messages about the selected device, the severity of the problem (error or warning), detailed descriptions for each message, and the steps you can take to resolve the problem.

#### Related Topics

- [Policy Discovery Status Page, page Q-2](#)
- [Viewing Policy Discovery Status Information, page 20-4](#)

## Viewing Policy Discovery Status Information

This procedure describes how to view the status of the policy discovery.

#### Procedure

- 
- Step 1** Select **Tools > Policy Discovery Status**. The Policy Discovery Status page appears. The Tasks pane displays the status of the overall task.
  - Step 2** Select a task from the Tasks pane. Corresponding information about that task is displayed in the Discovery Details pane or Import Details pane, whichever applies.
  - Step 3** Select a device from the Discovery Details pane or Import Details pane. Corresponding information about that device is displayed in the Messages text box.
  - Step 4** Click a message row. Detailed information about that message is displayed in the Description text box.
  - Step 5** Look at the Action field for steps to resolve the problem.

For information about the elements in the Policy Discovery Status page, see [Policy Discovery Status Page, page Q-2](#).

---

#### Related Topics

- [Understanding Show Containment, page 20-5](#)
- [Policy Discovery Status Page, page Q-2](#)

# Understanding Show Containment

The Show Containment option displays information about composite devices. If you select this option, the containment of a device, that is, the service modules and security contexts supported on the selected device, is displayed:

**Note**

---

This option is available for Catalyst 6500/7600, FWSM, PIX Firewall 7.0, and ASA devices.

---

- For Catalyst 6500/7600 devices, displays the IDSM and FWSM service modules, and the security contexts supported by the FWSM.
- For FWSMs, displays security contexts supported by the FWSM.
- For PIX Firewalls, displays security contexts supported by the PIX Firewall.
- For ASA devices, displays security contexts supported by the ASA device.

For information about security contexts, see [Configuring Security Contexts on Firewall Devices, page 15-105](#).

This procedure describes how to view the containment of a device.

**Procedure**

- 
- Step 1** Select a Catalyst 6500/7600, PIX Firewall 7.0, FWSM, or ASA device from the Device selector.
- Step 2** Select **Tools > Show Containment**.
- The Composite View opens and displays containment information on the selected device.
- 

**Related Topics**

- [Configuring Security Contexts on Firewall Devices, page 15-105](#)

# Understanding Inventory Status

Security Manager provides a summary of device properties for all devices that you are authorized to manage. The summary includes device contact information and all device configurations, indicating which settings are local, which are used a shared policy, and indicate any policy object overrides in effect.

The report is in table format, allowing you to organize information by filtering, sorting, and reordering and removing columns. You can also export the table contents to a CSV file in the Security Manager server file system.

This procedure will help you view and customize device summary information:

## Procedure

---

- Step 1** Select **Tools > Inventory Status**. The Inventory Status appears. For more information on the fields in this page, see [Table Q-4 on page Q-6](#).
  - Step 2** To view a subset of the devices listed, select a filter from the Filter list, or you can create a filter. For more information, see [Filtering Tables, page 3-24](#).
  - Step 3** Use the scroll buttons to highlight the device for which you wish to view data.
  - Step 4** To generate a CSV file on the Security Manager server:
    - a.** Click **Export**. The Export Inventory Status dialog box appears.
    - b.** Select a directory for the CSV file in the left pane of the Export Inventory Status window.
    - c.** Enter a name for your file in the File name field.
    - d.** Click **OK**. The CSV file will be generated and ready to retrieve on the server.
- 

## Working With Device OS Management

Security Manager integrates several key features from Resource Manager Essentials (RME). You can use software management to analyze individual device operating systems versions (also known as image versions) and generate image

analysis reports. This then allows you to import and distribute operating system images to groups of devices. Operating system upgrade jobs can also be scheduled to ensure up-to-date versions and minimize errors.

Software Image Management (SWIM) includes the following features:

- **Software Repository**—Determines the images that are missing from the network, imports these images into the software library, keeps the library up-to-date, and periodically synchronizes the library with the images running on the network devices. You can also schedule an image import for a later, more convenient time, as well as download an appropriate image from Cisco.com.
- **Software Distribution**—Generates upgrade analysis reports that allow you to determine prerequisites for image upgrade. You can either select a set of devices and perform an image upgrade, or select a software image and select a set of devices on which to perform the upgrade.
- **Software Management Jobs**—Allows you to view, edit, stop, or delete scheduled image upgrade jobs.

For a detailed description of the fields on this page, see [Device OS Management Page, page A-16](#). The following features are all cross launch points to RME features:

- Using the Software Repository
- Understanding Software Distribution
- Scheduling Management Jobs

For more information consult the context sensitive online help available on these pages, or the RME user guide online at <http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html>.

## Understanding Audit Reports

When state changes occur in Security Manager, an audit entry is created in the audit log. You can display the aggregated results of the audit entries by defining the parameters in the Audit Report page. 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 for 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.
- Admin changes, such as workflow on and workflow off modes.
- Changes to the state of Security Manager objects:
  - Activity changes, such as creating, editing, submitting, and approving an activity.
  - Deployment changes, such as creating, editing, and submitting a deployment job.
- Changes to the state of managed devices:
  - Object changes, such as changes to building blocks.
  - Inventory changes, such as adding, deleting, modifying devices in the inventory.
  - Policy changes, such as creating, restoring, modifying, and deleting policies.
  - VPN changes, such as creating, modifying, and deleting a VPN.

Before you generate the audit report, you can narrow your search criteria by defining the parameters for the report in the Audit Report page. The Audit Report page contains two panes. You define the parameters in the left pane and click Search to display the audit report, corresponding to the parameters you defined, in the right pane.

The following topics provide more information:

- [Guidelines for Defining the Audit Report Parameters, page 20-9](#)
- [Generating the Audit Report, page 20-9](#)
- [Viewing Audit Logs, page 20-10](#)
- [Purging Audit Log Entries, page 20-11](#)

## Guidelines for Defining the Audit Report Parameters

The following examples provide some guidelines that will help you understand what parameters you should define to get the information you need:

- To find out the deployment history of device X—From the Search by action column, select **Deployment > Create**. In the **Search by all or part of the object name** field, enter the name of the device. In this instance, enter **X**, then click **Search**.
- To find out when the device X was removed from Security Manager management—From the **Search by action** column, select **Devices > Delete**. In the **Search by all or part of the object name** field, enter the name of the device. In this instance, enter **X**, then click **Search**.
- To find out if a failed login attempt occurred in the system—From the **Search by action** column, select **System > Authorization > Login > Failed**, then click **Search**.

### Related Topics

- [Understanding Audit Reports, page 20-7](#)
- [Generating the Audit Report, page 20-9](#)
- [Audit Report Page, page Q-8](#)

## Generating the Audit Report

You narrow down your search criteria by defining the parameters for the audit report in the Audit Report page.

This procedure describes how to generate an audit report.

### Procedure

- 
- Step 1** Select **Tools > Audit Report**. The Audit Report page appears.
  - Step 2** Enter the information in the required fields in the left pane. For more information, see [Table Q-5](#).
  - Step 3** Click **Search** to generate the audit report.

The audit report is displayed in the right pane. For more information, see [Table Q-6](#).

- Step 4** For a detailed description, double-click a row. The Audit Message Details page appears. For elements in this page, see [Audit Message Details Dialog Box](#), page Q-11.
- 

#### Related Topics

- [Understanding Audit Reports](#), page 20-7
- [Guidelines for Defining the Audit Report Parameters](#), page 20-9
- [Viewing Audit Logs](#), page 20-10

## Viewing Audit Logs

Audit logs are stored in two locations, in the Security Manager database and in the CiscoWorks Common Services database.

To view the audit logs in the Security Manager database, see [Generating the Audit Report](#), page 20-9.

To view the archived audit logs in Common Services, go to: CSCOPx/MDC/Logs/audit/ on the server machine or use the following procedure.

This procedure describes how to view audit logs in Common Services.

#### Procedure

---

- Step 1** Select **Common Services > Device and Credentials > Reports**. The Report Generator page appears.

- Step 2** Select **Audit Report**.

- Step 3** Enter the report range in the fields provided, then click **Generate Report**.

The generated report contains all audit logs from both Common Services and Security Manager.

---

**Related Topics**

- [Understanding Audit Reports, page 20-7](#)
- [Generating the Audit Report, page 20-9](#)

## Purging Audit Log Entries

To prevent database overload, the following audit log parameters have factory-set defaults:

- Time—60 days.
- Maximum number of entries—10,000 entries.

When the time limit or the maximum number of entries limit is reached, the audit logs that have expired are purged (deleted) from the system. To change the factory-set defaults, select **Tools > Security Manager Administration > Preferences > Logs**. For more information, see [Logs Page, page A-30](#).

**Related Topic**

- [Understanding Audit Reports, page 20-7](#)
- [Audit Report Page, page Q-8](#)
- [Viewing Audit Logs, page 20-10](#)
- [Logs Page, page A-30](#)

## Using the Configuration Archive Tool

Configuration Archive stores configuration versions for each device managed by Security Manager.

**Note**

---

Security Manager does not support the archiving of VLAN configurations.

---

You can use Configuration Archive to:

- View the transcript of a configuration deployment for a selected device.
- View and compare configuration versions.
- View CLI differences between deployed configuration versions.

- Rollback to an earlier configuration version that originated from the device.
- Retrieve a current device configuration.

You must have the proper permissions to access all of these features. For more information on permissions, see [Default Associations Between Permissions and Roles in Security Manager](#), page 2-32.



---

**Note** Configuration Archive differs from Preview Configuration which displays proposed configuration changes to the CLI. For more information on the Preview Configuration functions, see [Previewing Configurations](#), page 18-43.

---

### Related Topics

- [Adding Configuration Versions from a Device to the Archive](#), page 20-23
- [Configuration Archive Window](#), page Q-12
- [Configuration Version Viewer](#), page Q-15
- [Customizing the Configuration Archive Toolbar](#), page 20-12
- [Defining Configuration Archive Settings](#), page 2-62
- [Using Rollback to Deploy Archived Configurations](#), page 20-15
- [Viewing and Comparing Configurations](#), page 20-14
- [Viewing Transcripts](#), page 20-13
- [Transcript Viewer Window](#), page Q-17

## Customizing the Configuration Archive Toolbar

In the right pane you can view and sort configuration file versions by version ID, creation date, creator, archival source, creation comment, and transcript. You can rearrange the column headings to appear in any order, and you can hide columns that you do not find useful.

This procedure will help you add or remove toolbar buttons.

### Procedure

---

- Step 1** Select **Tools > Configuration Archive** to go to Configuration Archive.
- Step 2** In the Device selector, click any device. The Security Manager Configuration Archive window populates with archived configuration versions. For a description of the fields in this page, see [Table Q-8 on page Q-14](#).
- Step 3** Right click the Configuration Archive toolbar and select **Show Columns**. A list of toolbar buttons appears. A checkmark indicates that the button appears on the toolbar. No checkmark indicates that the button does not appear.
- Step 4** Select buttons to include or deselect buttons to exclude from the toolbar.
- 

### Related Topics

- [Adding Configuration Versions from a Device to the Archive, page 20-23](#)
- [Configuration Archive Window, page Q-12](#)
- [Defining Configuration Archive Settings, page 2-62](#)
- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Viewing and Comparing Configurations, page 20-14](#)
- [Viewing Transcripts, page 20-13](#)

## Viewing Transcripts

A transcript is the log file of Security Manager server and device transactions captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of deployment or rollback request. If rollback is unsuccessful, there might be a partial transcript generated depending on which stage rollback or deployment failed.

This procedure will help you view transcripts.

### Procedure

---

- Step 1** Select **Tools > Configuration Archive** to go to Configuration Archive.

In the Device selector, click the device for which you want to view a transcript. The Security Manager Configuration Archive window populates with archived configuration versions for the device you selected. For a description of the fields in this page, see [Table Q-8 on page Q-14](#).

- Step 2** Double-click the **Transcript** icon next to the configuration version for which you want to view its transcript. The transcript for that configuration version appears.
- 

### Related Topics

- [Transcript Viewer Window, page Q-17](#)
- [Adding Configuration Versions from a Device to the Archive, page 20-23](#)
- [Configuration Version Viewer, page Q-15](#)
- [Customizing the Configuration Archive Toolbar, page 20-12](#)
- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Viewing and Comparing Configurations, page 20-14](#)

## Viewing and Comparing Configurations

You can view and compare any one full configuration version to any other in the archive from the configuration version viewer. You can view a delta configuration file from this viewer as well. A delta configuration file is generated by Security Manager during deployment and represents policy changes between the existing configuration and the one currently being deployed. Delta configuration versions contain command syntax different from that for full configuration versions, and include negation commands. A delta configuration file is available only for configuration versions in the archive that have been deployed to a device by Security Manager. When available, these can be viewed from the configuration version viewer.

This procedure will help you view and compare configurations.

### Procedure

---

- Step 1** Select **Tools > Configuration Archive** to go to Configuration Archive.

In the Device selector, click the device for which you want to view a full or delta configuration version. The Security Manager Configuration Archive window populates with archived configuration versions for the device you selected. For a description of the fields in this page, see [Table Q-8 on page Q-14](#).

**Step 2** Select the configuration version that you want to view or compare and click **View**.



---

**Tip** If you are comparing configuration versions, you only need to select one of the two in the version list.

---

The configuration version viewer opens. The configuration version you selected is in the left pane of the configuration version viewer. For details on interpreting the color coding in the file versions, and using the change indicator buttons, see [Configuration Version Viewer, page Q-15](#).

**Step 3** To compare configuration versions, select a different version from the Compare with version list. The version you selected appears in the right pane of the configuration viewer.

**Step 4** To view the delta configuration for the version in the left pane, from the Config Type list select the (Delta) configuration. For details on interpreting the color coding in the file versions, and using the change indicator buttons, see [Configuration Version Viewer, page Q-15](#).

---

#### Related Topics

- [Adding Configuration Versions from a Device to the Archive, page 20-23](#)
- [Viewing Transcripts, page 20-13](#)
- [Configuration Version Viewer, page Q-15](#)

## Using Rollback to Deploy Archived Configurations

You can roll back any configuration version, from Configuration Archive to the device for which it is archived, provided that the configuration originated from the device. You cannot roll back to a file configuration. The rolled-back configuration then becomes another archived version in the list for that device.

This procedure will help you roll back to an archived configuration.

### What happens during rollback

On PIX/ASA/FWSM devices, Security Manager uses the replace config option on the device's SSL interface to perform the equivalent of a reload (xlates are cleared, IPsec tunnels are torn down, and so on).

For routers running IOS 12.3(7)T or later, Security Manager uses the **configure replace** command to replace the running configuration with the contents of a configuration file. Support for this command is dependent on the IOS version installed on the router:

- On routers running IOS 12.3(7)T or later, Security Manager copies the configuration file to the startup configuration before executing the **configure replace** command. If the configure replace operation fails, Security Manager issues the **reload** command to reload the operating system using the contents of the startup configuration. Please note that the **reload** command restarts the system, which might result in a temporary network outage.
- On routers running a version prior to 12.3(7)T, Security Manager copies the configuration file to the startup configuration and issues the **reload** command.



#### Note

Special considerations apply to the rollback of certain device types and configurations. Please see the following sections for more information:

- [Understanding Rollback for Devices in Multiple Context Mode, page 20-18](#)
- [Understanding Rollback for Failover Devices, page 20-18](#)
- [Understanding Rollback for Catalyst 6500/7600, page 20-19](#)
- [Understanding Rollback for IPS and IOS IPS, page 20-19](#)
- [Commands that Can Cause Conflicts after Rollback, page 20-22](#)
- [Commands to Recover from Failover Misconfiguration after Rollback, page 20-23](#)

### Procedure

- Step 1** Select **Tools > Configuration Archive** to go to Configuration Archive.

In the Device selector, click the device for which you want to roll back a different configuration version. The Security Manager Configuration Archive window is populated with archived configuration versions for the device you selected. For a description of the fields in this page, see [Table Q-8 on page Q-14](#).

**Step 2** Highlight the device by clicking the device name.

**Step 3** Highlight the configuration version to deploy to device.

**Note**

---

You can roll back only to a configuration that originated from the device. You cannot roll back to a file configuration.

---

To view the configuration version before rollback, click **View**. For a description of the fields in this page, see [Table Q-9 on page Q-16](#).

**Step 4** Click **Rollback** to deploy the selected configuration version to the selected device. A progress box appears, followed by a notification message when the configuration version is successfully deployed. An error message appears if the deployment was not successful.

---

**Related Topics**

- [Adding Configuration Versions from a Device to the Archive, page 20-23](#)
- [Configuration Version Viewer, page Q-15](#)
- [Managing Deployment, page 18-1](#)
- [Viewing and Comparing Configurations, page 20-14](#)
- [Understanding Rollback for Devices in Multiple Context Mode, page 20-18](#)
- [Understanding Rollback for Failover Devices, page 20-18](#)
- [Understanding Rollback for Catalyst 6500/7600, page 20-19](#)
- [Understanding Rollback for IPS and IOS IPS, page 20-19](#)
- [Commands that Can Cause Conflicts after Rollback, page 20-22](#)
- [Commands to Recover from Failover Misconfiguration after Rollback, page 20-23](#)

## Understanding Rollback for Devices in Multiple Context Mode

If the configuration of the system context to which you are rolling back specifies connectivity options to security contexts (for example, *vlan config*) and there is a mismatch between the configuration selected for rollback and the current running configurations of the security contexts, Security Manager might not be able to connect to the security contexts. In such cases, we recommend that you roll back configurations for the security contexts before rolling back a configuration for the system context.

**Note**

---

If you roll back a configuration for the system context of a device in multiple context mode to one that includes a different set of security contexts, after rollback the security contexts on the device might not match the security contexts managed by Security Manager that appear in the Device selector.

---

**Related Topics**

- [Using Rollback to Deploy Archived Configurations](#), page 20-15
- [Commands that Can Cause Conflicts after Rollback](#), page 20-22
- [Commands to Recover from Failover Misconfiguration after Rollback](#), page 20-23

## Understanding Rollback for Failover Devices

If you roll back a configuration that contains a failover policy, a switchover could occur during rollback or connectivity between the active and standby units might be lost. To prevent problems, please copy the bootstrap configuration to the standby unit after rollback completes. For more information, please see [Bootstrap Configuration for LAN Failover Dialog Box](#), page L-127.

**Related Topics**

- [Using Rollback to Deploy Archived Configurations](#), page 20-15
- [Commands that Can Cause Conflicts after Rollback](#), page 20-22
- [Commands to Recover from Failover Misconfiguration after Rollback](#), page 20-23

## Understanding Rollback for Catalyst 6500/7600

If you roll back a configuration to a Catalyst 6500/7600 device that specifies connectivity options to service modules (for example, *vlan config*) and there is a mismatch between the configuration selected for rollback and the current running configuration, Security Manager might not be able to connect to the service modules. We recommend that you roll back configurations for the service modules before rolling back a configuration to the Catalyst 6500/7600 chassis.

### Related Topics

- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Commands that Can Cause Conflicts after Rollback, page 20-22](#)
- [Commands to Recover from Failover Misconfiguration after Rollback, page 20-23](#)

## Understanding Rollback for IPS and IOS IPS

Special considerations apply to the rollback of IPS devices and IOS IPS devices. For IPS devices and IOS IPS devices, rollback could possibly include rolling back sensor updates or signature updates. The reason for this is that for IPS devices and IOS IPS devices, Security Manager supports not only the management of configuration but also the support of image management in the form of manual and automatic upgrades and signature updates.

Rollback is accomplished through Configuration Archive. For IPS devices and IOS IPS devices, only the current configuration is archived. The current configuration for one device version (say, Version X) may not be valid for a different device version (say, Version Y). Security Manager rolls back a configuration of Version X to a sensor with Version Y as long as the configuration for X is valid for Y.

If the configuration for X is valid for Y, rollback proceeds and Security Manager displays a confirmation dialog box to you. If the configuration for X is not valid for Y, Security Manager displays a warning dialog box to you and provides you with the option of downgrading the sensor during rollback if such a downgrade will help accomplish the rollback.

**Caution**

Downgrading an IPS device removes certain capabilities of the IPS device. For example, downgrading the engine prevents you from applying the latest signature updates. Operation of an IPS device without the latest signature updates diminishes the effectiveness of the IPS device.

For rollback of a deployment job, the warning dialog box contains one or more of the following types of warnings:

- Security Manager warns you about IPS devices that need to have their sensor version downgraded before a rollback can be performed.
- Security Manager warns you about IOS IPS devices whose signature level has changed. For these devices, only the non-IPS sections of the configuration can be rolled back.
- Security Manager warns you about IPS devices that must be downgraded more than one level, and as a result, Security Manager cannot do it. You must use the Cisco IPS CLI for such downgrades. The warning dialog box displays the version to which the device must be reimaged or downgraded.

**Note**

The option of downgrading an IOS IPS device during rollback is not available, because IOS IPS devices do not support downgrade.

If the option of downgrading the sensor during rollback will not help accomplish the rollback, you receive an error message stating that rollback cannot occur and that you need to manually reinstall the image on the device to roll back. Only the update package most recently installed on a device can be downgraded, so downgrade does not help in the following cases:

- Rollback of a deployment (signature update) that involves downloading more than one update package to the device.
- Selection of an old deployment or configuration for rollback subsequent to which several upgrades occurred.
- Rollback of an upgrade that cannot be downgraded. Major, minor, and most service pack upgrades cannot be downgraded, as shown in [Table 20-1](#)

For rollback of a configuration that requires a downgrade to a version prior to Cisco IPS 5.1(4), Security Manager does not support automatic downgrade. You must manually downgrade the device to the specified version and then proceed with rollback.

**Table 20-1** Downgrade Support for Possible Sensor Upgrade Types

| Upgrade Type  | Downgrade Support   |
|---|---|
| Major Upgrade   | Downgrade is not supported.                                     |
| Minor Upgrade   | Downgrade is not supported.                                     |
| Service Pack Update   | Downgrade from Cisco IPS 5.1(4) onward is not supported.        |
| Patch update  | Downgrade is supported.   |
| Signature Update  | Downgrade is supported.   |
| Engine Update   | Downgrade is supported.   |
| Repackage (applicable to major, minor, and service pack updates). | Repackages for service packs prior to 5.1(4) can be downgraded. |

**Caution**

Outbreak Prevention updates on a particular device may be lost if that device is downgraded.

Out-of-band changes discovered during rollback result in Security Manager taking the actions listed in [Table 20-2](#).

**Table 20-2** Result of Out-of-Band Changes Discovered During Rollback

| Out-of-Band Condition   | Action Taken by Security Manager   |
|---|--|
| During rollback, Security Manager discovers that there have been out-of-band changes to the device that prevent rollback. | Security Manager displays an error message stating that out-of-band changes prevent rollback |

**Related Topics**

- [Using Rollback to Deploy Archived Configurations, page 20-15](#)

## Commands that Can Cause Conflicts after Rollback

The following commands can potentially cause conflicts after rollback is performed:

- *http server enable <port>*  
*http <ip\_address> <net\_mask> <interface\_name>*  
Applicable only to security contexts (not system context).
- *allocate-interface <physical\_interface -or- subinterface> [map\_name] visible | invisible]*  
Applicable only to the system context under the context subcommand.
- *config-url <diskX:/path/filename>*  
Applicable only to the system context under the context subcommand.
- *join -failover-group <group\_number>*  
Applicable only for active/active failover and only to the system context under the context subcommand. The failover group defaults to group 1 if not specified.
- *failover*  
Applicable only to system context. Enabling “failover” causes configuration synchronization to trigger between peers.
- *failover lan enable*  
Applicable only to system context. If this command is omitted, this implies serial cable failover on a PIX platform or warrants an incomplete failover configuration warning on ASA and FWSM.
- *failover lan unit <primary | secondary>*  
Applicable only to system context. If this command is not specified, both units are secondary by default. If rollback takes place on wrong unit, both can become primary which impacts which unit becomes active initially.
- *failover group <group\_number>*  
Applicable only to system context. This command enables active/active failover. If this command is omitted, active/standby is enabled.

- *preempt <delay>*

Applicable only to system context and under the failover group subcommand to force which failover group becomes active if both units are booted up at the same time, or the primary does not boot up within the ‘delay’ specified.

- *monitor-interface <interface\_name>*

Applicable only to security contexts and used to enable health monitoring of critical interfaces. If this interface is ‘bounced’ or fails, a switchover could occur.

#### Related Topics

- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Commands to Recover from Failover Misconfiguration after Rollback, page 20-23](#)

## Commands to Recover from Failover Misconfiguration after Rollback

If a switchover happens during rollback and the two units are no longer synchronized, you might need to use the following commands to recover:

- *failover active <group\_number>*
- *failover reset <group\_number>*
- *failover reload-standby*
- *clear configure failover*

For more information on these commands, please refer to the command reference for your security appliance.

#### Related Topics

- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Commands that Can Cause Conflicts after Rollback, page 20-22](#)

## Adding Configuration Versions from a Device to the Archive

Configuration Archive is updated any time a configuration version is rolled back to a device, in the form of a new line item in the archive for the device to which you rolled back.

You can retrieve a configuration directly from the device to add to the Configuration Archive. This is useful when changes have been made directly to device configurations (out-of-band changes outside the scope of Security Manager).

**Note**

---

Configurations cannot be retrieved from those devices that are managed by AUS, and have been configured with dynamic IP addresses.

---

This procedure will help you retrieve a configuration from a device and add it to the archive for that device.

**Procedure**

- 
- Step 1** Select **Tools > Configuration Archive** to go to Configuration Archive.
- In the Device selector, click the device for which you want to retrieve its running configuration. The Security Manager Configuration Archive window populates with archived configuration versions for the device you selected. For a description of the fields in this page, see [Table Q-8 on page Q-14](#).
- Step 2** Click **Add from Device**. The configuration version is added to the list of configuration versions in Configuration Archive.
- Step 3** Locate the Creation Comment next to the version you just added to verify the new version was added. Time, date, and userid appear in this column.

**Note**

---

You will receive a notification message if the retrieval was successful, and an error message if it was not.

---

**Related Topics**

- [Configuration Version Viewer, page Q-15](#)
- [Using Rollback to Deploy Archived Configurations, page 20-15](#)
- [Viewing and Comparing Configurations, page 20-14](#)

# Apply IPS Update

The Apply IPS Updates wizard allows you to *manually* apply image and signature updates to compatible IPS devices. For step-by-step details on the Apply IPS Updates wizard, refer to [Apply IPS Update, page Q-18](#).

*Automatic* updates can be configured via **Tools > Security Manager Administration > IPS Updates**. For details on automatic updates, refer to [IPS Updates Page, page A-19](#).

# Backup and Restore

You can backup and restore the Security Manager database using Common Services. From the Backup page you can schedule immediate, daily, weekly, or monthly automatic backups. This is accessible from the Tools menu by selecting **Tools > Backup**. For more information, click **Help** from the Common Services Backup page. Restoration of Security Manager database and data files is supported only by running a script on the command line.

A procedure for backup and restore is documented in Common Services documentation. We strongly recommend you take a backup of your current system before restoring an older backup. For information and a procedure on restoring the database, please see [http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_common\\_services\\_software/3.0/user/guide/admin.html#wp257472](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_common_services_software/3.0/user/guide/admin.html#wp257472).



---

**Note**

While backing up and restoring data, both Common Services and Security Manager processes will be shutdown and restarted.

---

You cannot restore a backup from an earlier version of Security Manager into Security Manager 3.1 if that backup contains any pending data, meaning data that has not been committed to the database. Before upgrading to a new version of Cisco Security Manager, we recommend committing or discarding all uncommitted changes and then creating 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**.




---

**Note** 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**.

---

**In Workflow mode:**

- To commit changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Submit**.




---

**Note** If you have enabled the activity approval requirement, you must also approve all activities after submitting. To approve an activity, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve**.

---

- To discard uncommitted changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

## Security Manager Diagnostics

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 reported problem. The Security Manager diagnostic tool is a utility that you can use to collect the diagnostic information from the Security Manager server. This tool is a plug-in for the MDCSupport utility provided by Common Services. The Security Manager diagnostic tool is invoked whenever you run the MDCSupport utility; it collects log files, configuration settings, memory info, complete system related

information, process status, and host environment information. It also collects any other relevant data into a tar (compressed form) file to support the security management applications installed.

The following topics describe how to gather troubleshooting information and to contact TAC for help:

- [Diagnostic Utility Executable Menu Item, page 20-27](#)
- [Generating a Diagnostic File from a Security Manager Client, page 20-28](#)
- [Generating a Diagnostic File from a Security Manager Server, page 20-29](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 20-29](#)

## Diagnostic Utility Executable Menu Item

You can use the diagnostic utility to run diagnostics on your system. A file with diagnostic information, CSMDiagnostics.zip, is generated and saved to a specified location on your server. This file is useful when working with the TAC to troubleshoot.

By default, the CSMDiagnostic.zip file is placed in the `<installation_location>/CSCOPx/MDC/etc` directory, where `<installation_location>` is the drive and directory in which you installed CiscoWorks Common Services (for example, `c:\Program Files`).

The CSMDiagnostic.zip file consists of:

- 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).

**Note**

---

There is no requirement to submit a CSMDiagnostics.zip file when you first submit a problem report. If Cisco requires the file, your support engineer tells you how to submit it.

---

You can run Security Manager Diagnostics in either of two ways:

- [Generating a Diagnostic File from a Security Manager Client, page 20-28](#)
- [Generating a Diagnostic File from a Security Manager Server, page 20-29](#)

## Generating a Diagnostic File from a Security Manager Client

This procedure will help you generate a diagnostic file for troubleshooting purposes from a Security Manager client.

### Procedure

---

**Step 1** Select **Tools > Security Manager Diagnostics** to begin file generation. The Security Manager Diagnostics dialog box appears.

**Step 2** Click **OK** to begin generating the diagnostics file. A Security Manager Diagnostics progress bar indicates the progress of the file generation.

When file generation is complete a confirmation dialog box indicates that the file has been created. It will say something like “Diagnostic file **CSMDiagnostic.zip** is generated in the directory C:\PROGRA~\CSCOPx\MDC\etc on the client *Security Manager client name*.”

**Tip**

---

We recommend that you rename this file so it will not get overwritten each time this utility is run.

---

## Generating a Diagnostic File from a Security Manager Server

This procedure will help you generate a CSMDiagnostics.zip file for troubleshooting from a Security manager server.

### Procedure

---

- Step 1** Select **Start > Run**, then enter **command**. Or, if your server keyboard includes a Windows key, press **Windows-R**, then enter **command**.
- Step 2** Enter **C:\Program Files\CSCOp\MDC\bin\CSMDiagnostics**. Or, to save the ZIP file in a different location than *NMSROOT\MDC\etc\*, enter **CSMDiagnostics drive:\path**. For example, CSMDiagnostics D:\temp.

The utility creates a tar file in the directory you specified.

Before you close the command window, ensure that the MDC Support utility has completed its action.

If you close the window prematurely, the subsequent instances of MDCSupport Utility will not function properly.

If you happen to close the window, delete the *mdcsupporttemp* directory from *NMSROOT\MDC\etc* directory, for subsequent instances to work properly.

---

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

