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

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.

Note A special consideration applies if you are using Internet Explorer 10.x in Windows Server 2012 (Standard or Datacenter)—64-bit, support for which is new in Version 4.7 of Cisco Security Manager. You need to be aware of this consideration when using the following navigation path: Windows Start > Cisco Security Manager Client > [log in] > Configuration Manager > Tools > Security Manager Administration... > Server Security. The Server Security page will open normally for you, but on that page you will be unable to use the buttons (e.g., Local User Setup) to cross-launch the Server Security Tools within Common Services. To work around this problem, decrease the security levels of your intranet settings in Internet Explorer 10.x.

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

Note The **Software Center > Software Update** feature in Common Services is not supported by Cisco Security Manager.

Managing a Cluster of Security Manager Servers

A Security Manager server cluster is two or more Security Manager servers used to manage a network. Typically, you want to maintain some relationship between the servers. Although there is no systematic relationship between the servers in the cluster, there are some techniques that you can use to maintain a cluster-like relationship. The topics in this section explain how you can manage a group of Security Manager servers as a cluster.

This section contains the following topics:

Overview of Security Manager Server Cluster Management

You can manage a large number of devices with a single Security Manager server. There are, however, a variety of reasons for managing your network with more than one Security Manager server. For example:

- If you have a very large network with thousands of devices to manage, you might find performance to be unacceptable when trying to manage all devices from a single server.
- For geographic reasons, you might find it better to have servers that are closer to managed devices. For example, if you have major sites on different sides of the globe, having separate servers at each major site might simplify management and improve performance. For example, when deploying configurations to managed devices, a Security Manager server located in Bangalore should be able to deploy configurations to a device in Bangalore much faster than a Security Manager server located in San Francisco simply due to the much shorter physical network distance.

- You might want to segment device management based on the technology managed. For example, you might want to use one server to manage your site-to-site VPNs, another server to manage ASA firewall and remote access VPN policies, and a third server to manage IPS.
- Separate IT organizations might be managing different parts of your network. Although you can set up ACS to fine-tune access control to the device level, you might instead find it simpler to have distinct Security Manager servers for each IT organization.

If you decide to install more than one Security Manager server, the main challenges are the following:

- Splitting a single server into two or more servers—You might currently have a single Security Manager server, and decide that you need multiple servers. For information on how to split a Security Manager server into two or more servers, see Splitting a Security Manager Server, page 10-3.
- Maintaining the same set of shared policies—If you use multiple servers to manage the same device types, you might want to ensure that the shared policies assigned to the devices are identical. For example, you might want to have the same set of mandatory and default access rules inherited by all ASA devices.

  There is no automatic process for maintaining the same set of shared policies among a cluster of servers. Instead, you must manually export them from your main server and import them into the remaining servers. For more information, see Synchronizing Shared Policies Among Security Manager Servers, page 10-5.

Splitting a Security Manager Server

If you decide that you need to convert a single Security Manager server into two or more servers, you can split the server by moving subsets of the devices managed by the original server to the new servers. Keep in mind that you should manage a specific network device from a single Security Manager server, so delete the moved devices from the original server.

Tip Use the same release of Security Manager software on all servers.

Related Topics

- Overview of Security Manager Server Cluster Management, page 10-2
- Synchronizing Shared Policies Among Security Manager Servers, page 10-5
- Exporting Shared Policies, page 10-12

Step 1 Install the new Security Manager servers as described in the *Installation Guide for Cisco Security Manager*.

Ensure that the server is functioning correctly, and also ensure that you install licenses with a device count that will be sufficient for the devices you will move to the server. Ensure that you use a professional license if you manage device types that require it. For information on installing licenses, see Installing Security Manager License Files, page 10-16.

Step 2 On the original server, verify that the policies of the devices that you will move will allow access from the IP address of the new server. For example, consider access rules on ASAs and routers, and the Allowed Hosts policy on IPS devices.

Step 3 On the original server, ensure that all configuration changes for the devices you are moving have been submitted and deployed. You will need to ask the staff to submit and deploy their changes, there is no simple way to determine this status within Security Manager.

This step ensures that there are no pending uncommited changes. For information on deploying configurations, see the following topics based on workflow mode:

- Deploying Configurations in Non-Workflow Mode, page 8-28
- Deploying Configurations in Workflow Mode, page 8-34

Step 4 Select **File > Export > Devices** to export the devices with their assigned policies and policy objects from the original Security Manager server. Be sure to select **Export Devices, Policies, and Objects** during the device export so that policy information is included. The file type must be **dev**. For more detailed information, see Exporting the Device Inventory from the Security Manager Client, page 10-6.

Create separate export files containing unique devices for each new Security Manager server.

Tip At this point, do not make policy changes to the exported devices in the original server, and do not deploy configurations to those devices. If you find that you need to make changes to the devices from the original server before you complete the split, create a new export file.

Step 5 On each of the new Security Manager servers, select **File > Import** to import the exported information to the new servers. For more detailed information, see Importing Policies or Devices, page 10-13.

Tip Device groups are not preserved during import. All devices are placed in the All group. You need to manually recreate the desired device group structure and add the devices to the appropriate groups.

Step 6 Verify that each of the new Security Manager servers can manage the newly-imported devices. For example, you could do a deployment, even for unchanged devices, to ensure that the new server can successfully contact all devices and deploy configurations.

Tip As explained in Importing Policies or Devices, page 10-13, you must submit policies before the changes are available for configuring devices. Submit policies before doing a deployment.

Step 7 If you were monitoring any of the moved devices using the original server (that is, with Event Viewer and optionally Report Manager), ensure that you update the relevant policies to have syslog messages sent to the new server and to allow contact from the new server. None of the event or report data from the original server is transferred to the new server.

For information on configuring the devices to enable Security Manager monitoring, see the following topics:

- Configuring ASA and FWSM Devices for Event Management, page 68-28
- Configuring IPS Devices for Event Management, page 68-29

Step 8 On the original Security Manager server, select **File > Delete Devices** to delete the moved devices from the original server. For information on deleting devices, see Deleting Devices from the Security Manager Inventory, page 3-57.

Synchronizing Shared Policies Among Security Manager Servers

When you have more than one Security Manager server, you can manually synchronize the shared policies among those servers. When you synchronize shared policies, the policy objects that are used by those shared policies are also synchronized.

Tips

- There is no programmatic way to identify a single Security Manager server as the "primary" server, the one that contains the official version of shared policies. You must decide which server to use as the primary and have the discipline to edit shared policies on that server only.
- Use the same release of Security Manager software on all servers.
- You can also synchronize certain types of policy object among servers even if those objects are not used in shared policies. If you have network/host, service, or port list objects that you want to synchronize, you can use the command described in Importing and Exporting Policy Objects, page 6-23.
- When importing shared policies and policy objects, the imported information always replaces any existing shared policies or policy objects of the same name. Therefore, if you allow users to create their own shared policies and objects on a server where you will import policies and objects, it is critical that you develop a policy and object naming standard so that user policies and objects are not accidentally overwritten by newly imported policies and objects.

Related Topics

- Overview of Security Manager Server Cluster Management, page 10-2
- Splitting a Security Manager Server, page 10-3
- Exporting the Device Inventory from the Security Manager Client, page 10-6

Step 1 On the original server, ensure that all configuration changes for the shared policies and policy objects have been submitted. You will need to ask the staff to submit their changes and have them approved, there is no simple way to determine this status within Security Manager.

When exporting shared policies, there is no need to ensure that new changes have been deployed to devices assigned to the policies. Device assignments and deployment status are not part of the exported information.

Step 2 Select **File > Export > Policies** to export the shared policies and any policy objects used by the policies. The export process creates a file with the extension **pol**.

Tip You cannot pick and choose which policies to export. You can select policy types only. All shared policies of a selected type are exported.

For more detailed information, see Exporting Shared Policies, page 10-12.

Step 3 On each of the other Security Manager servers, select **File > Import** to import the exported shared policy information to the servers. For more detailed information, see Importing Policies or Devices, page 10-13.

Tip Any shared policies or objects that have the same name as imported ones are replaced. The import of a policy or object will fail if a user already has a lock on the policy or object. As explained in Importing Policies or Devices, page 10-13, you must submit policies before the changes are available for configuring devices.

Step 4 If you do not want to import all of the shared policies, delete the ones you did not want to import on the other servers. This is a manual process.

Exporting the Device Inventory

Exporting the device inventory allows you to import the inventory into other network management applications, or to manipulate the output for your own reporting purposes. There are two unrelated methods to export the device inventory:

- Use the **File > Export > Devices** command—Using this command, you can create either a simple comma-separated values (CSV) file, or a compressed .dev file that contains the devices along with their complete configuration policies. The CSV file is in a format suitable for importing into the CiscoWorks Common Services Device Credential Repository (DCR), the Cisco Security Monitoring, Analysis and Response System (CS-MARS), Cisco Prime Security Manager (PRSM), or another Security Manager installation; or you can open it and view it in a spreadsheet or text editor program. The .dev file is suitable for importing into another Security Manager server only. For more information, see Exporting the Device Inventory from the Security Manager Client, page 10-6.
- Use the CSMgrDeviceExport Perl script—Using this Perl script, you can export the inventory without starting the Security Manager client. You can direct the output to the screen or to a comma-separated values (CSV) file. For more information, see Exporting the Device Inventory from the Command Line, page 10-10.

Note Only the five most recent versions of each device configuration are exported.

Exporting the Device Inventory from the Security Manager Client

You can export the device inventory in a variety of formats. These are the main choices:

- **Export as CSV** (comma-separated values)—You can create a simple CSV file containing inventory information in one of the following formats: CSM (for use with Cisco Security Manager), Device Credential Repository (DCR, for CiscoWorks Common Services), and CS-MARS seed file (for use with Cisco Security Monitoring, Analysis and Response System). You can open a CSV file in a spreadsheet application or text editor, and use the file with any application that supports the format, including other Security Manager servers. However, this format contains no policy information, so if you use it with another Security Manager server, you must discover policies while adding the devices.
  - For more information about the CSV formats, see Supported CSV Formats for Inventory Import/Export, page 10-9.
  - For information on how to import devices from a CSV file, see Adding Devices from an Inventory File, page 3-31.

- **Export Devices, Policies, and Objects**—Export the device inventory along with all device properties, policies, and policy objects used by the device. Exported information includes the following:

  Note Importing of *.pol or *.dev files is only supported on the same version of Cisco Security Manager as used when exporting those files. You cannot export from one version of Cisco Security Manager and import on a server running a different version.

  - All local and shared policies assigned to the devices, including all policy objects used in the policies and any device-level overrides for the objects. Shared policy assignments are maintained.
  - Device properties and inventory.
  - Configuration Archive data for the devices.
  - History snapshots for the devices.
  - Device certificates.
  - IPS device license and certificate information. Applied signatures are not exported (when importing the device, you must have the same signature package registered on the server). IPS update settings are not included; you will have to recreate them after import.
  - The VPN topologies in which the devices participate. However, a VPN topology is exported only if all devices that participate in the topology are included in the export. Extranet VPNs are always exported.

  Thus, the export file includes the complete policy configuration for the selected devices. The file created has the extension .dev and can be read only by another Security Manager server (the file contents are compressed and uninterpretable, which preserves the security of your policy information).

  For information on importing a .dev file into another Security Manager server, see Importing Policies or Devices, page 10-13.

Export Size Limitations

If your Security Manager database contains a large number of devices or a large number of policies or policy objects, you should limit the number of devices you export at one time to prevent errors. The following guidelines can be used to help estimate the number of devices you can successfully export at one time:

Example 1: 1000+ devices in the database with approximately 1500+ polices per device and approximately 25,000 objects in the database:

- Maximum number of devices (devices only) to be exported at one time = 250
- Maximum number of devices (along with polices and objects) to be exported at one time = 100 to 150

Example 2: Fewer than 1000 devices in the database with approximately 1500+ polices per device and approximately 10,000-15,000 objects in the database:

- Maximum number of devices (devices only) to be exported at one time = 250 to 300
- Maximum number of devices (along with polices and objects) to be exported at one time = 200

Tips

- When you select the **Export Devices, Policies, and Objects** option, you can export to the Security Manager server or to the local Security Manager client. When exporting a CSV file, you can only export to the Security Manager server. You can control the ability to export to or import from the local Security Manager client from **Tools > Security Manager Administration > Customize Desktop**. For more information, see Customize Desktop Page, page 11-10.
- Exported devices are not deleted from the inventory. If you intend to manage the devices from a different Security Manager server, delete the devices after successfully importing them into the other server.
- If you select a device that uses an AUS or Configuration Engine to manage its configuration, you should also select the server in the list of devices to export. You cannot export AUS or Configuration Engine information in CS-MARS format.
- You can export unmanaged devices.
- When exporting devices with their policies, only policies and policy objects that have been submitted and approved are included in the export file. Make sure that all desired submissions and approvals have occurred before exporting devices with policies and policy objects.
- No type of export file includes event and report data (that is, data that is available through Event Viewer or Report Manager). Thus, if you are exporting devices with the intention of moving them to another Security Manager server, the event and report data that was already collected for the device will not be available on the new server.
- No type of export file includes device group information. You will have to manually recreate device groups and assign devices to them after importing devices.
- When selecting security contexts or virtual sensors, be sure to select the host device as well. Also, if a device is part of a VPN, ensure that you select all devices in the VPN when exporting devices, policies, and policy objects.
- When selecting IPS or IOS IPS devices, make sure that you have already applied an IPS signature update to the device. Although you can export an IPS or IOS IPS device with the base sensor package (Sig0), you will not be able to import it. The import error will be “missing Sig0 package.”
- When you select the following types of device that are contained in another device, the hosting device is also automatically exported: any module in a Catalyst 6500/7600, an AIM or NME module in a router. You can separately export ASA devices and their IPS modules.
- You cannot export devices with their policies (.dev format) while an activity or configuration session is being approved. All approvals must be complete before you can export devices with policies. In Workflow mode with an approver, contact the approver and ask that the approval be completed in a timely manner. In non-Workflow mode, or Workflow mode without an approver, wait a few minutes before retrying the export, because approvals happen automatically when changes are submitted.
- While you are exporting devices with their policies (.dev format), policy changes cannot be approved. Once the export file has been created, and the command finishes, users can again approve policy changes. In non-Workflow mode, or Workflow mode without an approver, this means that submissions are not allowed during the export process.
- To export devices, policies, and policy objects, you must have Modify Policy and Modify Object privileges to the policy and object types, and Modify Device privileges. These privileges can be assigned for separate policies, objects, and devices when using ACS for authorization control. Having system administrator, network administrator, or security administrator privileges provide the required privileges.

  When exporting devices to CSV, you need Modify Devices privileges only.

Related Topics

- Filtering Items in Selectors, page 1-45
- Selecting or Specifying a File or Directory in Security Manager, page 1-50
- Customize Desktop Page, page 11-10

Step 1 In Device view, select **File > Export > Devices** to open the Export Inventory dialog box.

Step 2 Select either **Export as CSV** or **Export Devices, Policies, and Objects**. These options are described above.

Step 3 Select the devices that you want to include in the export file and click **>>** to add them to the Selected Devices list. You can select a folder to select all devices in the folder.

The list from which you choose contains only those devices to which you have Modify Device permissions.

Note If your Security Manager database contains a large number of devices or a large number of policies or policy objects, you should limit the number of devices you export at one time to prevent errors. For more information, see **Export Size Limitations** above.

Step 4 Click **Browse** to select the folder in which to create the export file and to enter a name for the file. For File Type, select the type of file that you want to create; this selection is critical when creating a CSV file, whereas there is a single option when creating a .dev file.

Click **Save** to return to the Export Inventory dialog box. The Export Inventory To field is updated with the export file information.

Step 5 Click **OK** to create the export file.

A message indicates when the export completes and whether there were errors in the export. When you click **OK**, if there are problems during the export, a dialog box opens listing the messages. If there is a Details button in the dialog box, you can select a message and click **Details** to see the message in a more readable format.

Supported CSV Formats for Inventory Import/Export

When you export devices to a CSV (comma-separated values) file (by selecting **File > Export > Devices** and selecting Export as CSV), or import devices from a CSV file (by selecting **File > New Device** and then selecting Add Device from File in the New Device wizard), you can select one of the following CSV file formats:

- **Device Credential Repository (DCR)**—The device management system for CiscoWorks Common Services. For information on this format, see the description of the sample version 3.0 CSV file in the Common Services documentation at this URL: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.3/user/guide/dcr.html#wp1193611
- **CS-MARS seed file**—Cisco Security Monitoring, Analysis and Response System. For information on this format, see the CS-MARS documentation at this URL: http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/device/configuration/guide/chDvcOver.html#wp162016

- **Cisco Security Manager**—The Security Manager format, which is the DCR version 3.0 format with additional fields. If you are importing the inventory into another Security Manager server, selecting this format will allow you to import the inventory without discovering policies on the devices.

  Note If the file does not specify os_type and os_version for a device, you must discover policies directly from the device when adding it.

  The additional fields, which appear at the end of each row, are:

  - os_type. The operating system type, which can be one of the following: PIX, ASA, IOS, FWSM, IPS. This field is required for all device types.
  - os_version. The target operating system version, which can be any of the version numbers listed in the New Device wizard when you select Add New Device. The acceptable version numbers differ depending on the device model, so if you are creating a CSV file by hand, look over this list carefully. For more information about adding devices using this method, see Adding Devices by Manual Definition, page 3-26. This field is required for all device types.
  - fw_os_mode. The mode in which a firewall device is running, which can be one of the following: TRANSPARENT, ROUTER, MIXED. This field is required for ASA, PIX, and FWSM devices.
  - fw_os_context. The context in which a firewall device is running, which can be one of the following: SINGLE, MULTI. This field is required for ASA, PIX, and FWSM devices.
  - anc_os_type. The ancillary operating system type for Cisco IOS-IPS devices. If present, it is IPS. This field is required for IOS IPS devices.
  - anc_os_version. The ancillary target operating system version, which is the IPS target operating system version. If present, it can be any of the supported IOS-IPS versions. This field is required for IOS IPS devices.

You can use these CSV files with any program that supports the file format. You can also create a CSV file yourself and use the file to import inventory into Security Manager.

Related Topics

- Exporting the Device Inventory from the Security Manager Client, page 10-6
- Importing Policies or Devices, page 10-13
- Adding Devices from an Inventory File, page 3-31

Exporting the Device Inventory from the Command Line

Security Manager includes a Perl script that you can use to export the device inventory without starting the Security Manager client. You can use this script to automate various offline reporting tasks that your organization might require. You can pipe the output to a comma-separated values (CSV) file or otherwise capture and manipulate the output.

Tip This command does not produce a file that you can use for importing devices or for adding devices "from file." Although it exports inventory information, making it similar to the integrated export features, the usefulness of the command is limited to reporting purposes for organizations that have unique off-line reporting process requirements.

The Perl command is located in $NMSROOT\bin, which is typically C:\Program Files\CSCSpx\bin. The syntax of the command is:

perl [*path*]**CSMgrDeviceExport.pl -u** *username* [**-p** *password*] [**-s** {**Dhdoirtg**}] [**-h**] [**>** *filename.csv*]

Syntax

perl [*path*] **CSMgrDeviceExport.pl**	The Perl script command. Include the path to the CSMgrDeviceExport.pl file if the path is not defined in the system path variable.
-u *username*	A Security Manager username. The data exported is limited by the permissions assigned to this user. The user must have View Device permissions.
-p *password*	(Optional.) The user's password. If you do not include the password on the command, you are prompted for it.
-s {**Dhdoirtg**}	(Optional.) The fields you are selecting to include in the output. If you do not specify the -s option, all fields are included. You can specify one or more of the following: • D—Display name. • h—Host name. • d—Domain name. • o—Operating system (OS) type. • I—Image name. • r—Running OS version. • t—Target OS version. • g—Device groups.
-h	(Optional.) Display the command line help. If you include this option, all other options are ignored.
> *filename.csv*	(Optional.) Pipe the output to the specified file. If you do not specify a file, the output is displayed on the screen.

Output Format

The output is in standard comma-separated values (CSV) format, which you can open in spreadsheet programs or process with your own scripts. The first line has column headings. The columns, left to right, are in the order of the fields described for the -s option above.

If there is no value for a particular field, that field is blank in the output.

The device group output field is enclosed in double-quotes and it can contain more than one group name. The group names include the path structure for the group. For example, the following output indicates the device is part of two groups, the East Coast group in the Department folder, and the NewGroup group in the New folder. Groups are separated by a semicolon.

```
"/Department/East Coast; /New/NewGroup"
```

Any error messages generated during the script are written to the output file.

Exporting Shared Policies

You can export shared policies and the policy objects that they use so that you can import them into another Security Manager server. This can help you maintain the same policies among a group of servers, as explained in Synchronizing Shared Policies Among Security Manager Servers, page 10-5.

Note Importing of *.pol or *.dev files is only supported on the same version of Cisco Security Manager as used when exporting those files. You cannot export from one version of Cisco Security Manager and import on a server running a different version.

Tips

- You can export to the Security Manager server or to the local Security Manager client. You can control the ability to export to or import from the local Security Manager client from **Tools > Security Manager Administration > Customize Desktop**. For more information, see Customize Desktop Page, page 11-10.
- Only shared policies and policy objects that have been submitted and approved are included in the export file. Make sure that all desired submissions and approvals have occurred before exporting policies.
- All policy objects referenced by shared policies are also exported. However, if a policy object is not referenced, it is not exported. There is a separate command you can use to export network/host, service, and port list objects directly; for information, see Importing and Exporting Policy Objects, page 6-23.
- You cannot export policies while an activity or configuration session is being approved. All approvals must be complete before you can export policies. In Workflow mode with an approver, contact the approver and ask that the approval be completed in a timely manner. In non-Workflow mode, or Workflow mode without an approver, wait a few minutes before retrying the export, because approvals happen automatically when changes are submitted.
- While you are exporting policies, policy changes cannot be approved. Once the export file has been created, and the command finishes, users can again approve policy changes. In non-Workflow mode, or Workflow mode without an approver, this means that submissions are not allowed during the export process.
- To export policies and their policy objects, you must have Modify Policy and Modify Object privileges to the policy and object types. These privileges can be assigned for separate policies, objects, and devices when using ACS for authorization control. Having system administrator, network administrator, or security administrator privileges provide the required privileges.

Related Topics

- Overview of Security Manager Server Cluster Management, page 10-2
- Splitting a Security Manager Server, page 10-3
- Synchronizing Shared Policies Among Security Manager Servers, page 10-5
- Exporting the Device Inventory from the Security Manager Client, page 10-6
- Selecting or Specifying a File or Directory in Security Manager, page 1-50
- Customize Desktop Page, page 11-10

Step 1 In Configuration Manager, select **File > Export > Policies** to open the Export Shared Policies dialog box.

Before opening the dialog box, Security Manager evaluates and loads any shared policies that are defined.

Step 2 Select the shared policies that you want to export, using any of the following methods:

Tip You can use multiple methods to select policies. For example, you can select all shared policies modified since a certain date and also select all shared policies of a specific type to export those policies in the same file.

- To select all shared policies that have been modified since a certain date, enter that date in the Modified since field and click **Select >>** next to the Modified since field. You can enter the date in *MMM DD YYYY* format or you can click the Calendar to select the desired date.
- To select all shared policies, select the **All** folder and click **Select >>** under Browse All Shared Policies.
- To select all shared policies of a specific type, select the shared policy type and click **Select >>** under Browse All Shared Policies. You can select a folder to move all types within the folder to the selected list.
- To specify specific shared policies to export, select the type of shared policies you want to export from the Browse All Shared Policies list, select the check boxes next to the shared policies of that type that you want to export, and then click **Select >>** to move them to the Selected Policies list. If you do not select any specific shared policies, all policies of the selected type will be added to the Selected Policies list.

Note Only those policy types for which shared policies have been defined are listed.

To remove any policies from the Selected Policies list, select them and then click the **<< Remove** button. Use the **Select All** checkbox to specify that all entries in the Selected Policies list are to be removed.

Step 3 Click **Browse** next to the Export Shared Policies To field to select the folder where the export file is to be created, and enter a name for the file. The file type is pre-selected as .pol; you cannot change the file type.

Click **OK** to save the file name and location.

Step 4 Click **OK** in the Export Shared Policies dialog box to begin the export. When the export is completed, you are told how many shared policies were exported and if there are warnings or errors, a dialog box opens listing the problems.

You can now import the policies into other Security Manager servers as explained in Importing Policies or Devices, page 10-13.

Importing Policies or Devices

You can import a shared policy (.pol) or device inventory plus policies (.dev) file that was exported from another Security Manager server.

Note Importing of *.pol or *.dev files is only supported on the same version of Cisco Security Manager as used when exporting those files. You cannot export from one version of Cisco Security Manager and import on a server running a different version.

Tips

- You can import from the Security Manager server or from the local Security Manager client. You can control the ability to export to or import from the local Security Manager client from **Tools > Security Manager Administration > Customize Desktop**. For more information, see Customize Desktop Page, page 11-10.
- When importing devices, the server must have a sufficient Security Manager license to support the number and types of devices that you are importing. Ensure that you install a professional license before importing device types that require it. For information on installing licenses, see Installing Security Manager License Files, page 10-16.
- When importing policies, whether during device or shared policy import, only the policy types selected for management on the Security Manager Administration Policy Management page will be visible. However, all policies are imported. If you select a previously deselected policy type for management, those imported policies appear with their imported configurations. For more information about selective policy management, see Customizing Policy Management for Routers and Firewall Devices, page 5-11.
- When importing shared polices and policy objects, if a policy or object on the server has the same name as an imported one, it is replaced by the imported policy or object. If there are locks on the policy or object, the import for that policy or object will fail. The message will indicate that the failure was due to a locking problem. To avoid problems, ensure that all users have submitted and approved any changes to shared policies or policy objects before doing an import.
- When importing devices, any shared policies and policy objects assigned to the device are also imported, and these policies and objects replace existing policies and objects under the same conditions as used when importing shared policies.
- To import policies and their policy objects, you must have Modify Policy and Modify Object privileges to the policy and object types. When importing devices, you must also have Modify Device privileges. These privileges can be assigned for separate policies, objects, and devices when using ACS for authorization control. Having system administrator, network administrator, or security administrator privileges provide the required privileges.
- You can import a file only if it was exported from a server running the same release of Security Manager.
- You cannot import a device if the device is already in the inventory. Thus, you cannot update device policies from an import file. If you want to re-import a device, first delete it from the inventory.
- When importing devices that use AUS or Configuration Engine servers to manage configuration deployment, the servers must either be included in the import file or already defined in the Security Manager server, but not both. You will get duplicate display name errors if the import file includes an AUS or Configuration Engine already defined in the inventory. You will get an “invalid server selection” error if you try to import a device that has an AUS or Configuration Engine server assigned to it, but the server is not included in the import file or defined in the inventory.
- You can import unmanaged devices.

- When importing IPS devices, the server must have the same signature levels as the imported devices. For example, if you import two IPS devices, one running signature level 481 and the other 530, you must have both 481 and 530 installed on the server. You might need to download signature packages before importing IPS devices as described in Checking for IPS Updates and Downloading Them, page 44-5.
- This procedure explains how to import .pol or .dev files. If you want to import a device inventory from a CSV file, the procedure is explained in Adding Devices from an Inventory File, page 3-31. The procedures are not similar.

Related Topics

- Overview of Security Manager Server Cluster Management, page 10-2
- Splitting a Security Manager Server, page 10-3
- Synchronizing Shared Policies Among Security Manager Servers, page 10-5
- Selecting or Specifying a File or Directory in Security Manager, page 1-50
- Customize Desktop Page, page 11-10

Step 1 In Configuration Manager, select **File > Import** to open the Import dialog box.

Step 2 Click **Browse** to select the file. Make sure that you select the desired file type (either .pol or .dev) from the Files of Type list on the Select a File dialog box.

Click **OK** when you have selected the file.

Step 3 Click **OK** in the Import dialog box.

You are warned that imported policies or policy objects will replace same-named policies and objects. If you have the required authorization privileges (system administrator or Modify Admin), you have the option to deselect **Display a warning on all shared policies and imported objects**. When selected, the banner for shared policies and imported objects warns users that shared policies might have been created during import, and that specific objects were in fact created during import. This warning provides notice that if the user changes the policy or object, those changes might be overridden by a subsequent policy import. Select whether you want to display a warning and click **Yes**.

Tip If you decide later that you want to change whether the warning is displayed, you can modify the **Display a warning on all shared policies and imported objects** option on the **Tools > Security Manager Administration > Policy Management** page.

The information is imported and you are informed of the results. If errors occur, nothing is imported and a dialog box opens that explains the errors. The most common errors include duplicate device display names when importing devices, or locks on shared policies or policy objects that have the same name as those being imported.

- To resolve the duplicate display name problem, you must delete the device from the inventory or rename it. You cannot selectively import devices, you must import all or none.

Note Not all duplicate device names might be listed. When using AUS or Configuration Engine to manage configuration deployment, imported AUS and Configuration names are evaluated before managed device names. Thus, you might see new duplicate display name errors after fixing the first set of errors.

- To resolve the locking problem, you must ensure that users submit their policy changes and have them approved. When importing devices, you might have to delete the imported devices before retrying the import.

Tip When importing devices, it might take some time for the devices to appear in the device list in Device view. Also, device groups are not preserved during import. All devices are placed in the All group. You need to manually recreate the desired device group structure and add the devices to the appropriate groups.

Step 4 Because policy changes are performed under an activity or configuration session, the imported policies and policy objects are not yet committed to the Security Manager database. You must submit and approve the changes. Based on Workflow mode:

- Non-Workflow mode—Select **File > Submit**.
- Workflow mode without an approver—Select **Activities > Approve Activity**.
- Workflow mode with an approver—Select **Activities > Submit Activity**. The activity must be approved before the changes are committed.

If you are not happy with the import, you can discard the activity or configuration session. However, when importing devices, the devices are added outside an activity or configuration session. Therefore, if you discard the activity or configuration session, you discard the device policies and VPN topologies, but the devices remain in the inventory. You should also delete the devices as described in Deleting Devices from the Security Manager Inventory, page 3-57.

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.

Three license types, Standard, Professional, and Upgrade, 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. Also see the *Installation Guide for Cisco Security Manager*.

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.

For non-evaluation licenses, if the database contains more devices than what is allowed by your configured licenses, you cannot log into the application using the Security Manager client. You are prompted to add a license during login, and login cannot complete until you add an appropriate 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 or upgrade license and any additional licenses that 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 or your local Security Manager client. If you are copying the license files to your 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.

  Note To install a license file that is located on your local Security Manager client, you must have client-side file browsing enabled (see Customize Desktop Page, page 11-10).

Tip Do not place the license file in the etc/licenses/CSM folder in the product's installation folder on the Security Manager server, 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.

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 11-57.

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. 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.

Certificate Trust Management

Cisco Security Manager downloads ASA images and IPS packages from Cisco.com over HTTPS, which uses certificates for establishing trust. Beginning with version 4.4, Security Manager has a certificate trust management feature. This feature helps you with improved handling of Cisco.com certificates for both types of downloads:

- ASA image downloads. For detailed documentation on certificate trust management for ASA image downloads, refer to Image Manager Page, page 11-41 or navigate to Tools > Security Manager Administration... > Image Manager > Help.
- IPS package downloads. For detailed documentation on certificate trust management for IPS package downloads, refer to Edit Update Server Settings Dialog Box, page 11-52 or navigate to Tools > Security Manager Administration... > IPS Updates > [Update Server group] > Edit Settings > Help.

Certificate Trust Management Feature

The certificate trust management feature in Security Manager has these characteristics:

- It behaves like a browser. It imparts trust to what you, as the user, consciously trust.
- It allows you to view the certificate and use your discretion in accepting it.
- It proactively validates a certificate to help you judge whether to accept or reject it. For example, it checks to see if a certificate is self-signed (not issued by a trusted Certificate Authority) and to see if it is expired, not yet valid, or revoked.
- After you accept a certificate, it stores that certificate on your Security Manager server.
- It provides transparency and control: You can retrieve and add a certificate, view a certificate, and remove a stored certificate.
- During communication with Cisco.com, it compares the live server certificate with the stored certificate and proceeds only upon a complete match. The complete certificate chain, not just the root certificate, is compared for a match. If there is a mismatch, the current operation is aborted until you view and accept the new certificate.
- It performs daily checks of your Security Manager server for certificate revocation and validity, and it removes any revoked or invalid certificates from your server. It does this by live contact with the CRL distribution points/URL present in the certificate. The default fixed schedule is for this daily check to be performed at 2:00 a.m.

Download Requirements

To download images from Cisco.com, you must retrieve, view, and accept both the latest image meta-data locator certificate and the latest certificate URL of the download site. The Security Manager interface has messages to assist you in key locations, and detailed documentation is available by referring to Image Manager Page, page 11-41 and Edit Update Server Settings Dialog Box, page 11-52.

Troubleshooting

During daily checks for certificate revocation and validity, the CRL revocation list is not stored on your Security Manager server. For that reason, if connectivity is lost, the daily checks fail to detect any possible certificate revocations. This problem will be solved after connectivity is restored.

If failure occurs while downloading ASA images or checking for IPS update packages, the most probable causes are the following:

- Site's certificate is not found on your Security Manager server

- There is a mismatch between the certificate received from the site and the stored certificate
- The site's certificate has expired

In all of these three cases listed above, the operation is aborted, and a message gives the cause of the error and the URL of the failed site. To recover, navigate to the user interface of the certificate feature (Tools > Security Manager Administration... > Image Manager or Tools > Security Manager Administration... > IPS Updates > [Update Server group] > Edit Settings); then retrieve, view, and accept the new certificate from the site and re-try the download.

If failure occurs while performing a check for IPS updates, verify that you have accepted both the certificate of the Cisco.com site used to obtain the meta-data information for IPS packages and the certificate of the actual download site of the IPS packages. Cisco recommends that you always configure email for notification of the job execution status. Then you can view the recommended actions in the email for recovering from the error. Copy the failed download URL from the email message to retrieve the certificate.

Because certificates are stored, if you upgrade to Security Manager 4.4 from a previous version, all communication with Cisco.com will fail. To resolve this problem, you must retrieve the certificates from the image meta-data locator and the download site URL.

If the stored certificate table in the user interface does not show the addition of a particular certificate, check to see if the daily checks for certificate revocation and validity have removed it because of revocation or expiration. You can do this by looking for the Certificate Revocation Check Task in the tomcat log; that log will enable you to determine the exact reason for the removal of the stored certificate.

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 **Manage > Audit Report**. The following topics provide more detailed information about audit reports:

- Understanding Audit Reports, page 10-19
- Generating the Audit Report, page 10-20
- Purging Audit Log Entries, page 10-23

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 **Manage > 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 10-20
- Purging Audit Log Entries, page 10-23

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 1-11.

Related Topics

- Understanding Audit Reports, page 10-19

Step 1 Select **Manage > 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 Using the Audit Report Window, page 10-21.

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.

Using the Audit Report Window

Use the Audit Report window to view records of state changes in Security Manager.

The Audit Report page contains two panes. Use the left pane to define the parameters for generating the audit report. The right pane displays the audit report using one row for each audit entry or message. The content of the audit report depends on the parameters you defined in the left pane. Therefore, all columns listed in the table might not be displayed in the generated audit report.

Navigation Path

Select **Manage > Audit Report**.

Related Topics

- Understanding Audit Reports, page 10-19
- Generating the Audit Report, page 10-20

Field Reference

Table 10-1 Audit Report Window

Element	Description
Search Criteria (Left Pane)	
The left side of the Audit Report window contains the search criteria for the report. The default report lists all state changes from yesterday and today, sorted with the most recent changes at the top.	
Search by action	One or more sources of actions to include in the audit report. If you do not make a selection, the report is not filtered based on action. You can select All to include all action sources.
Search by date	The time period to include in the report. Actions that occur between the from and to dates are displayed. Click the calendar icon to select the dates. This filter's default (reset position) is to include actions from yesterday to today.
Search for activity by state	This field works differently from the other search fields, and is primarily of use in Workflow mode. You can use this field to select one or more activities to include in the report. The activities are listed in the display box below the drop-down list. The drop-down list helps you find the activities on which you want to report. To use this search mechanism, select the activity state of the activities on which you want to report, and then select the activities. Use Ctrl+click to select multiple activities. Select No Activity to not filter by activity.

Table 10-1 Audit Report Window (Continued)

Element	Description
Search by message warning level	The message warning level. The report is limited to messages of the selected severity. Use Ctrl+click to select multiple levels.
Search by user name	The username of the person who performed the actions to include in the report. To see Security Manager system-generated actions, enter the username System.
Search by a phrase in the message body	A string of text that should occur in the message of the audit report entries. You can enter a maximum of 1025 characters. The message is not visible in the report table. To see the messages related to an entry, double-click the entry.
Search by all or part of the object name	A string of text that should occur in the name of the object for which the audit entries were generated. You can enter a maximum of 1025 characters.
Search button	Click this button to generate the report in the right pane.
Reset button	Click this button to reset the search criteria and delete any values or selections you made.
Audit Report (Right Pane)	
The right side of the Audit Report window contains the audit report. Each row represents one audit entry. Double-click a row to open the Audit Message Details dialog box, where you can view a more readable layout of the information and to see the specific messages associated with the entry. You can scroll through the entries in the report from within the Audit Message Details dialog box.	
Message Level	The message warning level: Information, Warning, Success, Failure and Internal System Error.
Date	The date and time the action occurred.
Source	The origin of the audit entry: Objects, License, Admin, Firewall, Policy Manager, Devices, Topology, VPN, Config Archive, Deployment, System, and Activity.
Action	The action performed: Add, Assign, Create, Delete, Open, Purge, Unassign, and Update.
Object	The identifier of the object of the action. For example, if the category is device, then the object identifier could be the device name or IP address. If the category is deployment, then the object identifier could be job name, job ID, and so on. There frequently is no specific object name.
User Name	The username of the person performing the action.
Activity	The name of the activity in which the action occurred, if any.
# of rows per page	The number of rows to display on each page.
< arrow	Click this button to return to the previous page of the audit report.
> arrow	Click this button to advance to the next page of the audit report.

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 11-62). 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.

Note The Purge Now button only removes audit report entries from the database. It does not remove the *.csv files from the ***<*install_dir*>**\CSCOpx\MDC\log\audit folder. These *.csv files can be deleted directly.

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 10-19
- Generating the Audit Report, page 10-20
- Using the Audit Report Window, page 10-21

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.

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 11-70).

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.

Changing Passwords for the Admin or Other Users

The admin user is a pre-defined user that has access to all Security Manager functions. When you install the product, you configure a password for the admin user. If you forget the password, you can use the following procedure to change it. You can also use this procedure to reset the password for other user accounts.

Step 1 Log into Windows on the Security Manager server and open a Windows command line window.

Step 2 Stop the daemon manager services by using this command:

net stop crmdmgtd

Tip You can also stop and start the daemon manager using the Services control panel.

Step 3 Run ResetPasswd.pl specifying admin as the user name. This example assumes you installed the product in the default directory; change the directory path if you used a different directory:

C:\Program Files\CSCOpx\bin\perl ResetPasswd.pl admin

You are prompted for a new password.

Tip If you want to change the password for a different user, replace **admin** with the desired user name.

Step 4 Start the daemon manager services by using this command:

net start crmdmgtd

Backing up and Restoring the Security Manager Database

You should regularly back up the Security Manager database in case you need to recover your work.

Tip The Security Manager database backup does not include the event data store used by the Event Manager service. If you want to back up event management data, see Archiving or Backing Up and Restoring the Event Data Store, page 68-35.

The following topics describe how to back up and recover the Security Manager database:

- Backing Up the Server Database, page 10-25
- Restoring the Server Database, page 10-27

Backing Up the Server 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.

After completing a backup, Security Manager compresses it. If you configure an e-mail address on the CiscoWorks Common Services backup page, you will get notifications of the completion of the backup and compression processes. If you have problems with file compression, or if you do not want to compress the backups, you can turn off backup compression. Edit the backup.properties file in the %NMSROOT%\conf folder (typically C:\Program Files\CSCOpx\conf) and change the backup compression property to specify NO instead of YES, as follows: VMS_FILEBACKUP_COMPRESS=NO.

Tip The backup includes the configuration and reporting databases, but it does not include the event storage areas. You can exclude the reporting database by changing the SKIP_RPT_DB_BACKUP property value to YES in the backup.properties file. Even if you specify YES, the backup will include reports generated by report schedules. For information on backing up the event data store, see Archiving or Backing Up and Restoring the Event Data Store, page 68-35.

While backing up and restoring data, both Common Services and Security Manager processes will be shut down and restarted. 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 “error 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 **Manage > Activities**. 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 **Manage > Activities**. From the Activity Manager window, select an activity and click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

You can also back up the database from a Windows command prompt using the following command:

[*path*]**perl** [*path*]**backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

Syntax

[*path*]**perl** [*path*]**backup.pl**	The Perl script command. Include the path to the perl command and the backup.pl file if the path is not defined in the system path variable. The typical path for both is C:\Progra~1\CSCOpx\bin\.
backup_directory	The directory where you want to create the backup. For example, C:\Backups.
log_filename	(Optional.) The log file for messages generated during backup. Include the path if you want it created somewhere other than the current directory. For example, C:\BackupLogs. If you do not specify a name, the log is %NMSROOT%\log\dbbackup.log.
email=*email_address*	(Optional.) The email address where you want notifications sent. If you do not want to specify an email address, but you need to specify a subsequent parameter, enter **email** without the equal sign or address. You must configure SMTP settings in CiscoWorks Common Services to enable notifications. For more information, see Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26.
number_of_generations	(Optional.) The maximum number of backup generations to keep in the backup directory. When the maximum is reached, old backups are deleted. The default is 0, which does not limit the number of generations kept.
compress	(Optional.) Whether you want the backup file to be compressed. If you do not enter this keyword, the backup is not compressed if VMS_FILEBACKUP_COMPRESS=NO is specified in the backup.properties file. Otherwise, the backup is still compressed. We recommend compressing backups.

Example

The following command assumes that you are in the directory containing the perl and backup.pl commands. It creates a compressed backup and log file in the backups directory and sends notifications to admin@domain.com. Note that you must specify a backup generation to include the compress parameter; if you specify any parameter after the log file parameter, you must include values for all preceding parameters.

```
perl backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress
```

Tip If you stop a backup that is in progress, you need to delete the backup.LOCK file in the Security Manager installation directory (typically C:\Progra~1\CSCOpx) before you can perform another backup.

Restoring the Server Database

You can restore your database by running a script from the command line. You have to shut down and restart CiscoWorks while restoring data. This procedure describes how you can restore the backed up database on your server. A single backup and restore facility exists to back up and restore all applications installed on a CiscoWorks server; you cannot back up or restore individual applications.

If you install the applications on multiple servers, ensure that you recover the database backup that contains data appropriate for the installed applications.

Tip You can restore backups taken from previous releases of the application if the backup is from a version supported for direct local inline upgrade to this version of the application. For information on which versions are supported for upgrade, see the *Installation Guide for Cisco Security Manager* for this release of the product.

Step 1 Stop all processes by entering the following at the command line:

net stop crmdmgtd

Step 2 Restore the database by entering:

*$NMSROOT***bin\perl** *$NMSROOT***bin\restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory*[**-h**]

where:

- *$NMSROOT*—The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).
- **-t** *temporary_directory*—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is *$NMSROOT*\tempBackupData.
- **-gen** *generationNumber*—(Optional.) The backup generation number you want to recover. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.
- **-d** *backup_directory*—The backup directory that contains the backup to restore.
- **-h**—(Optional) Provides help. When used with -d BackupDirectory, help shows the correct syntax along with available suites and generations.

For example, to restore the most recent version from the c:\var\backup directory, enter the following command:

C:\Progra~1\CSCOpx\bin\perl C:\Progra~1\CSCOpx\bin\restorebackup.pl -d C:\var\backup

Tip If you are restoring a database that contains RME data, you might be asked if you want to collect inventory data. Collecting this data can take a long time. You might want to respond No and then configure RME to schedule an inventory. In RME, select **Devices > Inventory**.

Step 3 Examine the log file, *NMSROOT***log\restorebackup.log**, to verify that the database was restored.

Step 4 Restart the system by entering:

net start crmdmgtd

Step 5 If you restore a database that was backed up prior to installing a Security Manager service pack, you must reapply the service pack after restoring the database.

Generating Data for the Cisco Technical Assistance Center

Cisco Technical Assistance Center (TAC) personnel might ask you to submit a variety of data to help them identify and resolve problems you might encounter when using the application. The following topics can help you generate the required information. However, you should perform these tasks only at the direction of the TAC, because the information is not always required to resolve a problem.

- Creating Diagnostics Files for the Cisco Technical Assistance Center, page 10-28
- Generating Deployment or Discovery Status Reports, page 10-30
- Generating a Partial Database Backup for the Cisco Technical Assistance Center, page 10-30

Creating Diagnostics Files for the Cisco Technical Assistance Center

Cisco Technical Assistance Center (TAC) personnel may ask you to submit system configuration information in the form of a diagnostics file when you submit a problem report. The diagnostics file assists them with diagnosing the problem. You do not need to submit a diagnostics file unless they ask you to.

Before you create the diagnostics file, perform the actions that lead to the problem in your report. If necessary, you can control the level of detail in the diagnostics file by changing the settings on the Debug Options page (**Tools > Security Manager Administration > Debug Options**); see Debug Options Page, page 11-11.

Beginning with Version 4.7, Cisco Security Manager supports diagnostics in a new, light variant; this "Light Diagnostics" variant collects only basic information; as a result, the diagnostics file is smaller, and its generation is faster. The existing "General Diagnostics" variant is the same in 4.7 as it was in 4.6 and earlier versions.

General Diagnostics File

The general diagnostics file (CSMDiagnostics.zip) contains the following files and information:

- 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)

To create CSMDiagnostics.zip by using the GUI, follow this procedure:

1. Using the Security Manager client, select **Tools > Security Manager Diagnostics... > General Diagnostics...**. A dialog box is opened.

2. Click **OK** to start the file generation. The dialog box displays the progress.
3. When the file is generated, click **Close**.

To create CSMDiagnostics.zip by using the CLI, follow this procedure:

1. Open a command line window on the Security Manager server.
2. Run the **~MDC\bin\CSMDiagnostics** program.
3. CSMDiagnostics.zip is placed in the <*installation_location*>/MDC/etc folder, where <*installation_location*> is the drive and directory in which you installed CiscoWorks Common Services. The default value for <*installation_location*> is C:\Program Files (x86)\CSCOpx.
4. If you want to, you can specify a different folder where CSMDiagnostics.zip is placed. For example, you can specify **CSMDiagnostics C:\Temp**.
5. You should move or rename CSMDiagnostics.zip after you create it, because it will be overwritten the second time you generate it, with only one previous version (appended with "_old") being saved.

Note When creating CSMDiagnostics.zip by using the CLI, you must allow the command to complete before closing the window; if you do not, subsequent attempts to run **CSMDiagnostics** 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.

Light Diagnostics File

The light diagnostics file (CSMDiagnostics_light.zip) contains a subset of the general diagnostics file (CSMDiagnostics.zip), so it is smaller and generated faster.

To create CSMDiagnostics_light.zip by using the GUI, follow this procedure:

1. Using the Security Manager client, select **Tools > Security Manager Diagnostics... > Light Diagnostics...**. A dialog box is opened.
2. Click **OK** to start the file generation. The dialog box displays the progress.
3. When the file is generated, click **Close**.

To create CSMDiagnostics_light.zip by using the CLI, follow this procedure:

1. Open a command line window on the Security Manager Server.
2. Run the following command: ***<installation_location>***\MDC\diagnostics\script>rundiag.bat, where <*installation_location*> is the drive and directory in which you installed CiscoWorks Common Services. The default value for <*installation_location*> is C:\Program Files (x86)\CSCOpx.
3. Be certain that you run the command with the following 3 parameters and in the order shown:

   3.1. Installation Folder—Folder where Security Manager server is installed. This must not be changed or modified. An error in the path leads to failure in the generation of the diagnostics file. Example: C:\PROGRA~2\CSCOpx\MDC

   3.2. Destination Folder—Folder where the diagnostics file will be placed after generation. You can specify any path and folder where you want the file to be saved. If you want the file to be saved in the default path, then you must specify the default path explicitly. If you do not specify the path, there will be an error in generation. Example: C:\PROGRA~2\Light_Diagnostics

   3.3. "LightDiagnostics" string without a space. The string alphabets are not case-sensitive, so you can use capital or lower-case letters, but you must not use a space in this string. If you neglect to specify this string, part of the general diagnostics (i.e., not light diagnostics) logs will automatically be collected in the destination folder.

4. Complete command screen example:

   C:\Program Files (x86)\CSCOpx\MDC\diagnostics\script>rundiag.bat
   C:\PROGRA~2\CSCOpx\MDC C:\PROGRA~2\Light_Diagnostics LightDiagnostics

Generating Deployment or Discovery Status Reports

You can generate status reports for deployment and policy discovery jobs. If you have problems involving deployment or discovery, these reports can help the Cisco Technical Support (TAC) personnel resolve your problem. Although the reports are mainly intended for troubleshooting, you can also generate these reports for your own uses.

The status reports are generated as Adobe Acrobat (PDF) files on your workstation (you are prompted to select the location to save the PDF file). The report includes a summary of the job and summaries for each device in the job. Deployment status reports also include the full and delta configurations and the transcript of communications between Security Manager and the device.

You can generate deployment or discovery reports in the following ways:

- **Deployment Status Reports**
  - When a deployment job finishes, either successfully or unsuccessfully, by clicking the **Generate Report** button on the Deployment Status dialog box. See Deployment Status Details Dialog Box, page 8-32.
  - For previously completed jobs, by selecting the job in the Deployment Manager and clicking the **Generate Report** button. See Deployment Manager Window, page 8-16.
- **Discovery Status Reports**
  - During a discovery job, which might occur when adding devices or when rediscovering policies on devices already in the inventory, by clicking the **Generate Report** button on the Discovery Status dialog box. See Discovery Status Dialog Box, page 5-23.
  - For previously completed jobs, by selecting the job in the Policy Discovery Status dialog box and clicking the **Generate Report** button. See Policy Discovery Status Page, page 5-25.

Generating a Partial Database Backup for the Cisco Technical Assistance Center

Caution This topic explains how to create a partial database backup. Partial backups are incomplete and you cannot use them as a replacement for full backups. Partial backups are strictly for use in troubleshooting and you should generate one only if instructed to do so by Cisco Technical Assistance (TAC) personnel.

Partial database backups have the same characteristics as regular backups, but they contain a more limited set of data. When creating a partial backup, you are asked whether you want to include data from the Configuration Archive, and if you say yes, how many archive versions (per device) you want to include (regular backups include the entire Configuration Archive). For a description of regular backups, see Backing Up the Server Database, page 10-25.

Tip The partial backup will include or exclude the reporting database based on the settings in the backup.properties file as described in Backing Up the Server Database, page 10-25.

While backing up and restoring data, both Common Services and Security Manager processes will be shut down and restarted. 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 "error loading page" in device policy windows. Note that if you try to restore a partial backup, the system will point out that it is a partial backup, and you will have to confirm that you want to restore a partial backup.

To generate a partial backup, use the following command at a Windows command prompt on the Security Manager server.

[*path*]**perl** [*path*]**partial_backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

Syntax

[*path*]**perl** [*path*]**partial_backup.pl**	The Perl script command. Include the path to the perl command and the partial_backup.pl file if the path is not defined in the system path variable. The typical path for both is C:\Progra~1\CSCOpx\bin\.
backup_directory	The directory where you want to create the backup. For example, C:\Backups.
log_filename	(Optional.) The log file for messages generated during backup. Include the path if you want it created somewhere other than the current directory. For example, C:\BackupLogs. If you do not specify a name, the log is %NMSROOT%\log\dbbackup.log.
email=*email_address*	(Optional.) The email address where you want notifications sent. If you do not want to specify an email address, but you need to specify a subsequent parameter, enter **email** without the equal sign or address. You must configure SMTP settings in CiscoWorks Common Services to enable notifications. For more information, see Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26.
number_of_generations	(Optional.) The maximum number of backup generations to keep in the backup directory. When the maximum is reached, old backups are deleted. The default is 0, which does not limit the number of generations kept.
compress	(Optional.) Whether you want the backup file to be compressed. If you do not enter this keyword, the backup is not compressed if VMS_FILEBACKUP_COMPRESS=NO is specified in the backup.properties file. Otherwise, the backup is still compressed. We recommend compressing backups.

Example

The following command assumes that you are in the directory containing the perl and partial_backup.pl commands. It creates a compressed partial backup and log file in the backups directory and sends notifications to admin@domain.com. Note that you must specify a backup generation to include the compress parameter; if you specify any parameter after the log file parameter, you must include values for all preceding parameters. Also note that you are asked whether you want to include the Configuration Archive, and if yes, how many archive versions to include in the backup. In this example, five archive versions per device are included in the backup.

```
perl partial_backup.pl C:\backups C:\backups\pbackup.log email=admin@domain.com 0 compress
```

```
Root: c:\backups
Do you also want to take config-archive backup(Yes/No): Yes
How many previous config-archive you want to restore: 5
```