



CHAPTER 4

Installing, Upgrading, Downgrading, Uninstalling, and Reinstalling Server Applications

This chapter contains these major sections:

- [Changing the Default Location for Temporary Files, page 4-2](#)
- [Exporting Data from IPS MC 2.2, page 4-3](#)
- [Installing Server Applications, page 4-4](#)
- [Upgrading Server Applications, page 4-8](#)
- [Retrieving Certificates After Upgrading from 3.0.1 to 3.1 Using Perl Scripts, page 4-11](#)
- [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 4-14](#)
- [Migrating IPS Sensors, page 4-16](#)
- [Importing IPS MC 2.2 Data, page 4-18](#)
- [Upgrading IPS Manager 3.0 Data, page 4-20](#)
- [Obtaining Service Packs and Point Patches, page 4-20](#)
- [Applying Service Packs and Point Patches, page 4-21](#)
- [Downgrading Server Applications, page 4-22](#)
- [Uninstalling and Reinstalling Server Applications, page 4-23](#)

Changing the Default Location for Temporary Files

The installation utility for Security Manager uses your Windows temporary directory, which Windows associates by default with your C:\ drive. If your target server has more than one local disk drive, and if you have less free space on your C:\ drive than is specified in [Server Requirements, page 2-5](#), you might edit the environment variables for your server so that C:\ is not the default location for temporary files.

To see the environment variables for your sever and edit their values so that you can change the default location for storing temporary files:

-
- Step 1** Right-click **My Computer**, then select **Properties** from the shortcut menu.
 - Step 2** Click the **Advanced** tab.
 - Step 3** Click **Environment Variables**.

The Environment Variables window contains one area for variables that are associated with the active username in the current login session, and another area for variables that always apply to your server. Both of these areas can include variables (with names like TEMP, TMP, and TMPDIR) that tell Windows and other software where to store temporary files.

- Step 4** Select the name of a variable that you want to change.
 - Step 5** Click **Edit**, change the value for that variable, then click **OK**.
-

Exporting Data from IPS MC 2.2

If you migrate data from an installation of IPS MC 2.2, and if the IPS MC server is the *same* server on which you install Security Manager, you must do the following *before* you start installing Security Manager.



Note

- We do not support Security Manager coexistence on the same server with VMS 2.3, the suite of applications of which IPS MC is one component. We recommend that you follow all the guidelines in [Chapter 3, “Preparing a Server for Installation.”](#)
 - Available space (on the IPS MC server disk partition where you will store your backup) must not be less than the size of the IPS MC database.
 - If the IPS MC database that you import contains Security Monitor sensor alarms or syslog events, Security Manager ignores those alarms and events when it imports the database. Security Manager cannot use any records that are associated with Security Monitor.
-

-
- Step 1** Back up your IPS MC server database files. See http://www.cisco.com/en/US/docs/security/security_management/vms/security_monitor/2.2/user/guide/DbRules.html#wp3263.
- Step 2** Move the backed-up database from CSCOpX\MDC\backup to a secure volume.
-

Installing Server Applications

**Tip**

To learn how to uninstall or reinstall Security Manager, see [Uninstalling and Reinstalling Server Applications, page 4-23](#).

You can install Security Manager 3.1 server software directly, or you can use the installation utility to upgrade the software on a server where an earlier Security Manager version is installed. For detailed information about upgrades, see [Upgrading Server Applications, page 4-8](#).

Before You Begin

- For supported OS versions, see [Server Requirements, page 2-5](#).
- We recommend that you install Security Manager on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of Security Manager and is not supported.
- Security Manager 3.1 requires that you use Common Services 3.0.5. Therefore, if you upgrade from an earlier Security Manager version, the installed Common Services version is also upgraded.
- If you obtained a base license for Security Manager (see [Effects of Licensing on Installation, page 1-8](#)), move a copy of the license file to your server. Security Manager sees only the local volumes, not the mapped drives, when you browse directories on your server.

- Step 1** Disable every application and process that uses any Sybase technology or software code, then follow the instructions that apply to your installation:

Installing from the DVD:	Installing from Cisco.com:
<p>Insert the <i>Security Manager</i> installation DVD in the Windows server DVD drive:</p> <ul style="list-style-type: none"> • If autorun is enabled, the installer opens automatically. • If autorun is not enabled, open the cs3_1_0_win_server folder, double-click Setup.exe, then click Yes to confirm that you are installing or upgrading Security Manager. 	<ol style="list-style-type: none"> Go to http://www.cisco.com/go/csmanager, then click Download Software. Download <i>both</i> the documentation and the self-extracting software installation utility for Cisco Security Manager 3.1. <p>Note Save the installation utility on a disk that is local to your server. Installation cannot succeed over a network connection to a remote volume, even if installation <i>seems</i> to succeed.</p> <ol style="list-style-type: none"> Print and read the documentation to learn what important considerations might affect your installation. Follow the instructions in the documentation for decompressing and starting the installation utility. <p>The InstallShield Wizard extracts files to a temporary directory and checks their integrity while it constructs the Cisco Security Manager Setup application, which starts automatically.</p> <p>Tip If an error message says the file contents cannot be unpacked, we recommend that you empty the Temp directory, scan for viruses, delete the C:\Program Files\Common Files\InstallShield directory, then reboot and retry. See also Changing the Default Location for Temporary Files, page 4-2.</p>

**Tip**

If you reinstall any applications, or install applications *in addition to* applications that you installed previously, or if you upgrade your installed applications, the Security Manager server performs a full, mandatory backup before you can advance beyond this step.

Step 2 When the Setup application prompts you to decide among essential options, such as which applications to install, select the options that meet your requirements.

If you do not understand your options, see the step-by-step instructions in [Appendix A, “Security Manager Server Installation GUI Reference.”](#)

**Note**

When the wizard prompts you to enter passwords for the admin login account and the System Identity login account, you must specify the same password for both accounts. See [Understanding User Accounts, page D-1.](#)

If you are installing Security Manager (rather than upgrading it), the installer prompts you to select your license options and enter your license key. You can use the free evaluation license or the base license file that you purchase.

If you use the Professional Edition of Security Manager (see [Effects of Licensing on Installation, page 1-8](#)), see the Performing Administrative Tasks section in the online help for information about installing any additional device license increments that you buy.

Step 3 Click **Finish**.

Setup installs and configures the selected components.

**Note**

If you are evaluating Security Manager, the evaluation period is 90 days and limits the maximum number of managed devices to 50. The evaluation version functions fully in all other ways. Each time that you start the evaluation version, a message is displayed that:

- Counts down the number of days remaining until the evaluation period ends.
- Tells you how to install a Security Manager license.

See [Effects of Licensing on Installation, page 1-8.](#)

Step 4 Restart the server.

Your Security Manager server is now:

- Available as a source from which to download the dedicated Security Manager client application. See [Chapter 5, “Installing or Uninstalling Security Manager Client.”](#)
- Protected by the standalone version of Cisco Security Agent. See [Cisco Security Agent, page 1-7](#), and see [Appendix C, “Cisco Security Agent: Standalone Agent Overview.”](#)

If you expect to import data from a preexisting installation of IPS MC, first see [Importing IPS MC 2.2 Data, page 4-18](#).



Caution

If McAfee VirusScan is installed on your server *and* if you will install RME or Performance Monitor now that Security Manager is installed, you *must* first:

1. Confirm that VirusScan is running.
2. Confirm that the VirusScan feature called “On-Access Scan” is running.

If VirusScan is installed but turned off, or if its On-Access Scan feature has been turned off, problems might prevent you from installing RME or Performance Monitor. In addition, any RME or Performance Monitor installations that fail for this reason might prevent Security Manager from operating correctly on your server. To work around these problems:

1. Reinstall Security Manager.
2. Start the VirusScan software.
3. Start the On-Access Scan feature in VirusScan.
4. Reinstall RME and Performance Monitor.

For information about the files that are installed on your server and the locations to which they are saved, see [Locations of Installed Files on Servers, page 1-11](#).

Upgrading Server Applications

**Note**

Security Manager 3.1 requires that you use Common Services 3.0.5. Therefore, if you upgrade from an earlier Security Manager version, the installed Common Services version is also upgraded.

Use the following procedure to upgrade the software on a server where Security Manager 3.0.x (or any of its related applications) is installed:

Step 1

Before you can successfully upgrade to Security Manager 3.1, you must make sure that the existing Security Manager database does not contain any pending data, meaning data that has not been committed to the database. If the existing Security Manager database contains pending data, you must commit or discard all uncommitted changes before upgrading:

- a. 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**.

- b. 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.

Step 2 Create a backup of the database for Security Manager 3.0.x. See “Using Tools > Backup and Restore” in the online help.



Note If network management applications, such as Tivoli, were used to install Cygwin on the same system where a Security Manager server was installed, backup of the Security Manager database fails.

Step 3 To upgrade in place, simply run the installer for Security Manager 3.1. For step-by-step instructions, see [Installing Server Applications, page 4-4](#).



Note When you upgrade in place to 3.1 from an earlier version of Security Manager and that version contains pending data, an error message is displayed stating that all pending activities must either be committed or discarded. If you get this error message, click **OK** to stop the installation, submit or discard all uncommitted data, and restart the installation. We recommend that you also create a backup of your current database after committing or discarding any pending data and before beginning the upgrade. For instructions on how to submit or discard uncommitted changes, see [Step 1](#).

When you upgrade in place from Security Manager 3.0.1 to Security Manager 3.1, the Auto Update Server 3.1 check box in the component selection screen of the installation wizard is grayed out and selected by default. As a result, AUS 3.1 is always installed on your server system, leaving you with no choice to deselect it during inline upgrade. Also, if Cisco Secure ACS was integrated with Security Manager before the upgrade, Auto Update Server is displayed in the Shared Profile Components and Group Setup pages of the CiscoSecure ACS interface after you complete the inline upgrade.

**Tip**

When the installer reaches its “Important Instructions” page, if you have used an earlier Security Manager version to manage Catalyst 6500 Series switches or Cisco 7600 Series routers, see [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 4-14](#), for important steps that we recommend you complete right now.

After you have completed the upgrade, skip to [Step 5](#).

Step 4 Alternatively, you can do the following:

- a. Uninstall Security Manager 3.0.x. See [Uninstalling Server Applications, page 4-23](#).

A version of Cisco Security Agent is installed on your Security Manager server. When you explicitly uninstall Security Manager, the Cisco Security Agent software remains on your server.

- If Cisco Security Agent is the fully configurable, commercial version, it will never be overwritten by a Security Manager installation or uninstallation.
- If Cisco Security Agent is the customized and standalone version, with predefined policies that you cannot change, it will be overwritten only when you install a new Security Manager version.

You can uninstall Cisco Security Agent manually, but we recommend that you do not. See [Uninstalling the Standalone Agent, page C-4](#).

- b. Install Security Manager 3.1. See [Installing Server Applications, page 4-4](#).

**Tip**

When the installer reaches its “Important Instructions” page, if you have used an earlier Security Manager version to manage Catalyst 6500 Series switches or Cisco 7600 Series routers, see [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 4-14](#), for important steps that we recommend you complete right now.

- c. Restore the database from its backup. See “Using Tools > Backup and Restore” in the online help.



Note If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.

Step 5 After you upgrade Security Manager, you must also uninstall Security Manager Client on every client system, then download and run the new version of the Security Manager Client installation utility. See [Chapter 5, “Installing or Uninstalling Security Manager Client.”](#)

Retrieving Certificates After Upgrading from 3.0.1 to 3.1 Using Perl Scripts

When you upgrade a Security Manager 3.0.1 server to 3.1 by backing up and restoring the database, the certificate thumbprints of the devices added to the Security Manager inventory are preserved in the 3.1 certificate data store if certificate authentication was enabled in 3.0.1. However, if did not enable certificate authentication in the 3.0.1 server, certificate validation for devices using SSL is disabled in 3.1 and device certificate thumbprints are not saved in the 3.1 certificate data store.

If you disabled certificate authentication for devices in 3.0.1 and want to enable certificate authentication for those devices after upgrading to 3.1, you can run perl scripts from the Security Manager server CLI to retrieve device certificates to the Security Manager certificate data store. You can either choose to retrieve certificate thumbprints and add them to Security Manager in a single step, or perform this operation using two separate scripts. The following two scripts enable you to add certificates to Security Manager quickly in bulk without having to manually retrieve them for each device.

- **getCerts.pl**—Exports device credentials to a .csv file from DCR and saves it at the specified location on the Security Manager server. You can use this script with the [-a] argument to add the exported credentials to the Security Manager certificate store, or add the certificates to Security Manager as a separate step by running the loadCerts.pl script.



Note Use the [-a] argument only if you trust the validity of the certificates retrieved from the devices.

- **loadCerts.pl**—Loads certificates to Security Manager from the CSV file generated using the getCerts.pl script.

After running these scripts to load certificates to the Security Manager certificate store, you can enable certificate authentication for the devices for which it is disabled from the Device Communication settings window.

To retrieve device certificates from live devices and add them to the Security Manager database after you upgrade to 3.1, follow these steps.

Before You Begin

- You must be logged in to Security Manager using the casuser account, equivalent to a Windows administrator, to run this script.
- To export device credentials using DCR, from the CiscoWorks home page, select **Common Services > Device and Credentials > Device Management**. You must select CSV as your output file format while exporting credential details. For more information, see the *User Guide for CiscoWorks Common Services 3.0.5*.
- Before you add the device certificate to Security Manager, check whether the certificate is authentic by verifying its attributes such as the validity period, end-host identity information, encryption keys that will be used for secure communications, and the signature of the issuing Certificate Authority. If you run the getCerts.pl script with the [-a] argument, you might want to verify the validity of the certificates before running the script because the certificates are automatically added to Security Manager at the end of running of the script.

Procedure

- Step 1** Open the Windows command prompt on the Security Manager server.
- Step 2** Navigate to the directory *NMSROOT\CSCOpX\bin*, where *NMSROOT* is the Security Manager installation directory. For example, enter **cd C:\Progra~1\CSCOpX\bin** if C:\Progra~1\CSCOpX\ is the directory where you installed Security Manager.

Step 3 Enter `getCerts.pl [-h] [-v] [-a] <input_csv_file> <output_cert_file>`

where:

- `[-h]`—(Optional) Displays the help associated with this utility, along with usage guidelines.
- `[-v]`—(Optional) Specifies verbose mode.
- `[-a]`—(Optional) Enables Security Manager to automatically obtain device certificates from live devices and load the thumbprints into the Security Manager certificate data store.
- `<input_csv_file>`—(Required) Specifies the name of the file to which a list of devices is exported from DCR in CSV format.
- `<output_cert_file>`—(Required) Specifies the location and name of the file in which device certificate details are saved.

If you run the `getCerts.pl` script without specifying the `[-a]` argument, you can view and modify the output file to remove certificate details for any device.

To load device certificates to Security Manager from the file to which they were exported from DCR using the `getCerts.pl` script, follow these steps.

Before You Begin

- If you ran the `getCerts.pl` script with the optional `[-a]` argument, the following procedure is not required because the certificates would have been already added to the certificate data store.
- If the Security Manager server is running when you execute the following script, the script tries to refresh the certificate cache.
- You must be logged in to Security Manager using the `casuser` account, equivalent to a Windows administrator, to run this script.

Procedure

Step 1 Open the Windows command prompt on the Security Manager server.

Step 2 Navigate to the directory `NMSROOT\CSCOpX\bin`, where `NMSROOT` is the Security Manager installation directory. For example, enter `cd C:\Progra~1\CSCOpX\bin` if `C:\Progra~1\CSCOpX\` is the directory where you installed Security Manager.

Step 3 Enter `loadCerts.pl [-h] [-v] [-a] <input_file>`

where:

- `[-h]`—(Optional) Displays the help associated with this utility, along with usage guidelines.
- `[-v]`—(Optional) Specifies verbose mode.
- `[-a]`—(Optional) Enables Security Manager to automatically obtain device certificates from DCR and load the thumbprints into the certificate data store.
- `<input_file>`—(Required) Specifies the name of the file generated by the `getCerts.pl` script and that contains device certificates. You must specify the same filename you entered in the `<output_cert_file>` argument while running the `getCerts.pl` script.

If a device cannot be reached from Security Manager, the certificate for that device is not retrieved when you run the `getCerts.pl` script. If you ran the script in verbose mode, the action performed by the script when connectivity to a device fails is displayed.

Migrating Catalyst 6500 and Cisco 7600 Chassis

Security Manager 3.1 differs significantly from earlier releases in its features for managing Catalyst 6500 Series switches and Cisco 7600 Series routers, as well as their associated services modules (blades) and security contexts. Earlier Security Manager versions used features from an embedded variant of CiscoView Device Manager, which this version does not include. This version offers greater integration with, and consistency with, other Security Manager features.

The installation utility for Security Manager automatically detects if an older Security Manager version is present on your server. In most cases, information from the older Security Manager database is added automatically to the new database as part of the process of upgrading to the newer Security Manager version. However, the new methods for managing 6500 Series and 7600 Series devices are different enough from the old methods that you must do more than simply install the newer Security Manager version, in order to manage these devices in your network.

Step 1 Upgrade from the older Security Manager version to the newer version. See [Upgrading Server Applications, page 4-8](#).

Catalyst 6500 Series switches, Cisco 7600 Series routers, their services modules, and their security contexts are migrated automatically, along with all associated VPN policies and firewall policies. However, old inventory information from earlier Security Manager versions is discarded—including, for example, the records of described interfaces and configured VLANs.

When the installation utility reaches its “Important Instructions” page, it specifies a location on your server from which to access a migration report file. In most cases, the location will be *NMSROOT\MDC\log\readme.txt*, where *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files\CSCOpX**.

Step 2 Open and print the migration report; it contains important information that you should read.

Step 3 Install the new Security Manager Client software version on a client system (see [Installing Security Manager Client, page 5-5](#)), then use that client system to log in to your upgraded Security Manager server.

Step 4 To use Device view, click the **Device View** button on the main toolbar.

You must use Device view, *not* Policy view.

In the device selection tree, a red X partially covers each of the icons that represent your 6500 Series and 7600 Series chassis, as well as the services modules and security contexts associated with those chassis, as a visual cue to indicate that inventory information is not yet available for them.



-
- Note**
- Until you complete this procedure, do not deploy any chassis, services module, or security context that uses a red X icon. If you try, the deployment will fail.
 - Other device lists in the Security Manager GUI (such as the lists for deployment and policy assignment) do not include *any* icons for these chassis, services modules, or security contexts.
-

Step 5 Click any red X icon in the device selection tree.

Security Manager contacts the live device and automatically retrieves its inventory information. The red X is cleared from the icon. The chassis, services module, or security context is now available to you for deployments from Security Manager.

Migrating IPS Sensors

Security Manager 3.1 differs significantly from earlier releases in its features for managing:

- Cisco Intrusion Prevention System (IPS) sensors:
 - Appliances
 - Switch modules
 - Network modules
 - Security Service modules (SSMs)
- Cisco IOS IPS devices:
 - Cisco IOS routers with IPS-enabled images
 - Cisco Integrated Services Routers (ISRs)

Earlier Security Manager versions used features from a helper application called IPS Manager, which this version does not provide. Instead, this Security Manager version has fully integrated IPS management features.

The installation utility for Security Manager automatically detects if an older Security Manager version is present on your server. In most cases, information from the older Security Manager database is added automatically to the new database as part of the process of upgrading to the newer Security Manager version. However, the new methods for managing Cisco IPS sensors and Cisco IOS IPS devices are different enough from the old methods that you must do more than simply install the newer Security Manager version, in order to manage these devices in your network.

-
- Step 1** Upgrade from the older Security Manager version to the newer version. See [Upgrading Server Applications, page 4-8](#).
- Cisco IPS sensors and Cisco IOS IPS devices are migrated automatically, along with all associated IPS platform policies. However, old inventory information from earlier Security Manager versions is discarded—including, for example, the configuration and tuning of IPS signatures.
- When the installation utility reaches its “Important Instructions” page, it specifies a location on your server from which to access a migration report file. In most cases, the location will be *NMSROOT\MDC\log\readme.txt*, where *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files\CSCOpX**.
- Step 2** Open and print the migration report; it contains important information that you should read.
- Step 3** Install the new Security Manager Client software version on a client system (see [Installing Security Manager Client, page 5-5](#)), then use that client system to log in to your upgraded Security Manager server.
- Step 4** To use Device view, click the **Device View** button on the main toolbar.
- You must use Device view, *not* Policy view.
- In the device selection tree, a red X partially covers each of the icons that represent your IPS sensors and Cisco IOS IPS devices, as a visual cue to indicate that inventory information is not yet available for them.



-
- Note**
- Until you complete this procedure, do not deploy any IPS sensor or Cisco IOS IPS device that uses a red X icon. If you try, the deployment will fail.
 - Other device lists in the Security Manager GUI (such as the lists for deployment and policy assignment) do not include *any* icons for these chassis, services modules, or security contexts.
-

Step 5 Click any red X icon in the device selection tree.

Security Manager contacts the live device and automatically retrieves its inventory information. The red X is cleared from the icon. The IPS sensor or Cisco IOS IPS device is now available to you for deployments from Security Manager.

Importing IPS MC 2.2 Data

Before You Begin

If you migrate data from IPS MC 2.2 to Security Manager 3.1, you can complete the following procedure successfully only *after* you:

1. Complete the procedure described in [Exporting Data from IPS MC 2.2, page 4-3](#).
2. Complete the Security Manager installation. See [Installing Server Applications, page 4-4](#).



Note

- If the IPS MC database that you import contains Security Monitor sensor alarms or syslog events, Security Manager ignores those alarms and events when it imports the data. Security Manager cannot use any records that are associated with Security Monitor.
 - When you import IPS MC data into Security Manager:
 - Do not use spaces anywhere in the path.
 - Do not use a path that is longer than 67 characters, including the drive letter and any backslash characters.
 - We recommend that available space on the server disk partition be at least twice the size of the database file that you import.
-

To transfer IPS MC 2.2 data to Security Manager 3.1:

-
- Step 1** Move to your Security Manager server a copy of the IPS MC backup that you saved on a secure volume.
 - Step 2** Note the full pathname of the newly transferred copy of your backup file.
Example: c:\backup_2.2\20070104135727
 - Step 3** Execute the perl script supplied with Cisco Security Manager to create a special file called the `IpsCredentialFile`. The `IpsCredentialFile` is an XML file with IPS credentials that CiscoWorks 3.1 can import via the Device Credentials Repository.
Example: c:\progra~1\cscopx\bin>
c:\progra~1\cscopx\mdc\bin\ExportIpsCredentials.pl
c:\backup_2.2\20070104135727 c:\IpsCredentials.xml
 - Step 4** Log in to your Security Manager server and open CiscoWorks.
 - Step 5** Navigate to Common Services > Device and Credentials > Device Management.
 - Step 6** Click the Bulk Import button. The Import Devices dialog box appears.
 - Step 7** In the Import File Name field, enter or browse to the `IpsCredentialFile` that you created earlier in this procedure.
 - Step 8** In the Format Selection field, select XML.
 - Step 9** Enter Scheduling and Job Info information as desired.
 - Step 10** Click the Import button. The data that you exported from IPS MC 2.2 are imported into the CiscoWorks Device Credential Repository. When adding an IPS device to Security Manager, select the “Add from DCR” option.
-

The time required to import IPS MC data varies according to the size of the database file and the percentage of its records that must be discarded because they are associated with Security Monitor.

Upgrading IPS Manager 3.0 Data

To transfer IPS Manager 3.0 or IPS Manager 3.0.1 data to Security Manager 3.1:

-
- Step 1** Log in to your Security Manager server.
- Step 2** Add your IPS devices to Security Manager using the “Add from DCR” option.
-

Obtaining Service Packs and Point Patches



Caution

Do not download or open any file that claims to be a service pack or point patch for Security Manager unless you obtain it from Cisco. Third-party service packs and point patches are not supported.

After you install Security Manager, you might install a service pack or point patch from Cisco Systems to fix bugs, support new device types, or otherwise enhance Security Manager.

- To learn when Cisco has prepared a new, regularly scheduled service pack, and to download any service pack that matters to you, open Security Manager, then select **Help > Security Manager Online**. Alternatively, point your browser to: <http://www.cisco.com/go/csmanager>.
- If your organization submits a Cisco TAC service request, TAC will tell you if an unscheduled point patch exists that might solve the problem you have described. Cisco does not distribute Security Manager point patches in any other way.

Service packs and point patches provide server support for client software updates and detect version level mismatches between a client and its server.

Applying Service Packs and Point Patches

After you choose to download and install a service pack or a point patch for your server, you must apply the equivalent software update to each of your client systems. See:

- [Patching a Server, page 4-21.](#)
- [Patching a Client, page 5-10.](#)

Patching a Server



Before you apply a service pack or a point patch to your server, you might choose to create a compressed ZIP archive of *NMSROOT/MDC*, where *NMSROOT* is the path to the Security Manager installation directory. (The default is **C:\Program Files\CSCOpX**.) Then, if the service pack or point patch that you apply is not right for your needs or you have technical difficulties when you apply it, you can ask that a Cisco technical support engineer use the MDC.ZIP archive to restore your server. See [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xiii](#), or see [Appendix B, “Troubleshooting.”](#)

- To learn how to obtain a service pack or point patch, see [Obtaining Service Packs and Point Patches, page 4-20.](#)
- The version number of the service pack or point patch that you apply to your server must be the same as the version number of the service pack or point patch that you apply to your client systems. See [Patching a Client, page 5-10.](#)
- For information about the files that are installed on your server and the locations to which they are saved, see [Locations of Installed Files on Servers, page 1-11.](#)
- If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.

For step-by-step instructions that help you to apply a downloaded service pack or point patch to your server, see the readme or other user documentation that accompanies the file.

To patch a client, see [Patching a Client, page 5-10.](#)

Downgrading Server Applications

Security Manager supports downgrading from release 3.1 to either release 3.0 or release 3.0.1 (including downgrades to IPS Manager and AUS), but only when you meet all of these conditions:

- You upgraded previously from the relevant release to release 3.1.
- You kept a copy of the backup that Security Manager created when you upgraded.
- You have the installation DVDs for both the old version and the new version.

To downgrade:

-
- Step 1** Uninstall Security Manager 3.1 and AUS 3.1. See [Uninstalling Server Applications, page 4-23](#).
 - Step 2** Install Security Manager 3.0 or 3.0.1 and (optionally) AUS 3.0. See [Installation Guide for Cisco Security Manager 3.0](#) on Cisco.com.
 - Step 3** (Optional) If you have an installation DVD for Security Manager 3.0 but not for 3.0.1, obtain the upgrade utility from <http://www.cisco.com/go/csmanager>, then upgrade from 3.0. to 3.0.1.
 - Step 4** Restore your database from its backup. See the Security Manager online help topic at Using Tools > Backup and Restore.



Note Your downgraded copy of Security Manager 3.0.x includes only the information that you saved *before* you upgraded to release 3.1.

Uninstalling and Reinstalling Server Applications

**Note**

- To learn which data files are essential to Common Services operation and understand how to create archives of that data, see the Common Services online help or read the documentation on Cisco.com.
- If you reinstall any applications, the Security Manager server performs a full, mandatory backup before you can continue.

To uninstall or reinstall applications on your server, see:

- [Uninstalling Server Applications, page 4-23](#)
- [Reinstalling Server Applications, page 4-25](#)
- [Uninstalling Cisco Security Agent, page 4-26](#)

Uninstalling Server Applications

**Caution**

A server that is infected with a virus might be unstable after you uninstall software from it and reboot. If your server is not stable after an uninstallation and reboot, we recommend that you scan it for viruses and other kinds of malware.

**Note**

The standalone version of Cisco Security Agent is not affected in any way if you uninstall Common Services, Security Manager, or AUS. You must uninstall the standalone agent separately. See [Uninstalling the Standalone Agent, page C-4](#).

Before You Begin

- We recommend that you back up copies of all essential data files from your server before you uninstall Security Manager. See the Security Manager online help topic at Using Tools > Backup and Restore.
- If any version of Windows Defender (which was known in its public beta test versions as both Microsoft AntiSpyware and Giant AntiSpyware) is installed, you must disable it before you try to uninstall Security Manager. Otherwise, the uninstallation application cannot run.

Step 1 Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager**.

Step 2 From the list of applications, select one or more applications to uninstall.

Step 3 Click **Next** twice.

The uninstaller removes the applications that you selected.



Note If a Windows command line prompt window is open in `\CSCOp\bin` when you uninstall server applications, the uninstaller cannot delete `\CSCOp\bin`. In this case, you can choose whether and how to delete the directory.

Step 4 *Only after you uninstall Security Manager, Common Services, and all their related applications, assuming that you choose to uninstall all server applications:*

- a. If a folder exists at `C:\Program Files\CSCOp`, either delete, move, or rename the folder.
- b. If the `C:\CMFLOCK.TXT` file exists, delete it.
- c. Use a Registry editor to delete these Registry entries before you try to reinstall Security Manager or any of its related applications:
 - `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager`
 - `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\MDC`



Tip Although no reboot is required, we recommend that you reboot the server after an uninstallation so that Registry entries and running processes on the server are in a suitable state for a future reinstallation.

**Note**

If the uninstallation causes an error, see the “Troubleshooting the Installation” chapter in *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Windows*: http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/appenda.html.

- Step 5** (Optional) If you disabled Windows Defender before uninstalling Security Manager, you can choose now whether to reenable it.

**Tip**

If you uninstalled Performance Monitor or any other supported CiscoWorks application that was not installed automatically when you installed Security Manager, you might see that a Windows shortcut for it is still visible in your Start > Programs menu. In this case, you can right-click the shortcut and select **Delete** from the shortcut menu.

Reinstalling Server Applications

Your server will perform a full and mandatory backup when you select the required options to reinstall any Security Manager-related applications.

If you install Common Services and Security Manager on a server, then reinstall Common Services later, you must also reinstall Security Manager.

**Note**

During reinstallation, you might see a warning message that says:

The application that you are installing requires new tasks to be registered with ACS. If you have already registered this application with ACS from another server, you do not need to register it again. However if you re-register the application, you will lose any custom roles that you had created earlier for this application in ACS.

In this case, see “CiscoWorks-ACS Task Registration During Upgrade and Re-installation” in *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Windows*, at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_common_services_software/3.0.5/installation/windows/guide/instl.html#wp1192068.

-
- Step 1** If you are reinstalling because a problem on your server corrupted your Security Manager database, you must run **restorebackup.pl**.
- Step 2** To reinstall one or more Security Manager server applications, see [Installing Server Applications, page 4-4](#).
-

Uninstalling Cisco Security Agent

See [Uninstalling the Standalone Agent, page C-4](#).