



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

This chapter contains these major sections:

- [Changing the Default Location for Temporary Files, page 1-2](#)
- [Exporting Data from IPS MC 2.2, page 1-3](#)
- [Installing or Upgrading Server Applications, page 1-3](#)
- [Importing IPS MC 2.2 Data, page 1-7](#)
- [Obtaining Service Packs and Point Patches, page 1-9](#)
- [Applying Service Packs and Point Patches, page 1-9](#)
- [Downgrading Server Applications, page 1-10](#)
- [Uninstalling and Reinstalling Server Applications, page 1-11](#)

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 1-4](#), 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, which automatically installs IPS 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 1, “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, IPS Manager ignores those alarms and events when it imports the database. IPS 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 or Upgrading Server Applications



Tip

To learn how to uninstall or reinstall Security Manager, see [Uninstalling and Reinstalling Server Applications, page 1-11](#).

You can install Security Manager 3.0.1 server software directly, or you can upgrade the software on a server where Security Manager 3.0 is installed.

**Note**

- In addition to the options that this procedure describes, you can:
 1. Create a backup of a Security Manager 3.0 database.
 2. Uninstall Security Manager 3.0.
 3. Install Security Manager 3.0.1.
 4. Restore the database from its backup.

To learn how to create and restore from a backup, see the Common Services online help.

- If you expect to upgrade from VMS to Security Manager, see http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/prod_bulletin0900aecd803ffd79.html. This bulletin explains how you can use your Cisco Software Application Support (SAS) contract number or Cisco Software Application Support plus Upgrades (SASU) contract number for VMS to order a free license for Security Manager in the Product Upgrade Tool (PUT).

Before You Begin

- For supported OS versions, see [Server Requirements, page 1-4](#).
- We recommend that you install Security Manager on a dedicated server in a controlled environment.
- Security Manager 3.0.1 requires that you use Common Services 3.0.4. Therefore, if you upgrade from Security Manager 3.0 to 3.0.1, Common Services is upgraded from 3.0.3 to 3.0.4.
- If you install Security Manager and its related applications on a server where you previously installed any version of Common Services earlier than 3.0.3, you must first uninstall the older version and uninstall every application that relies on that version. If you install Security Manager on a server where any unsupported, older version of Common Services is installed, Security Manager might not work correctly. See [Chapter 1, “Preparing a Server for Installation.”](#)
- If you obtained a base license for Security Manager and IPS Manager (see [Effects of Licensing on Installation, page 1-7](#)), 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 active instance of Sybase, 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_0_1_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.¹ Download <i>both</i> the documentation and the self-extracting software installation utility for Cisco Security Manager 3.0.1. <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 1-2.</p>

1. RME is not included in the downloadable version of the installation utility. See [Resource Manager Essentials](#), page 1-5.

**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 A-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 1-7](#)), 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 1-7.](#)

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 1, “Installing or Uninstalling Security Manager Client.”](#)
- Protected by the standalone version of Cisco Security Agent. See [Cisco Security Agent, page 1-6](#), and see [Appendix A, “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 1-7](#).



Note

If you upgrade from Security Manager 3.0 to 3.0.1, 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 1, “Installing or Uninstalling Security Manager Client.”](#)

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 1-9](#).

Importing IPS MC 2.2 Data

Before You Begin

If you migrate data from IPS MC 2.2 to IPS Manager 3.0, you can complete the following procedure successfully only *after* you:

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

**Note**

- If the IPS MC database that you import contains Security Monitor sensor alarms or syslog events, IPS Manager ignores those alarms and events when it imports the data. IPS Manager cannot use any records that are associated with Security Monitor.
- When you import IPS MC data into IPS 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 IPS Manager 3.0:

-
- 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.
 - Step 3** From a Windows command line prompt in the *NMSROOT*\bin directory, run **IpsMcDbUpgrade.pl**, where *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files\CSCOpX**.

The command line argument to use includes the full pathname of the backup file; for example: `IpsMcDbUpgrade.pl D:\backup\20060104184347\ids-mdc`

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.

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 1-10](#).
- [Patching a Client, page 1-9](#).

Patching a Server



Tip

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.

- To learn how to obtain a service pack or point patch, see [Obtaining Service Packs and Point Patches, page 1-9](#).
- 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 1-9](#).
- 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 1-9](#).

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 1-9](#).

Downgrading Server Applications

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

- You upgraded previously from release 3.0 to release 3.0.1.
- You kept a copy of the backup that Security Manager created when you upgraded.
- You have the installation DVDs for both releases.

To downgrade:

-
- Step 1** Uninstall Security Manager 3.0.1 and AUS 3.0. See [Uninstalling Server Applications, page 1-12](#).
- Step 2** Install Security Manager 3.0 and (optionally) AUS 3.0. See [Installation Guide for Cisco Security Manager 3.0](#) on Cisco.com.
- Step 3** 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 includes only the information that you saved *before* you upgraded to release 3.0.1.

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 1-12](#)
- [Reinstalling Server Applications, page 1-13](#)
- [Uninstalling Cisco Security Agent, page 1-14](#)

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 A-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\CSCOPx, 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 3.0.3 (Includes CiscoView) on Windows*.

- 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.

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.

Select **Yes** if you have not already registered the application (on this or another server) with ACS. If you have already registered the application, if you select **Yes**, you will lose any customized user roles configured in ACS for the application, so you should select **No**. All Security Manager and AUS servers that use the same ACS server share user roles.

-
- 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 or Upgrading Server Applications, page 1-3](#).
-

Uninstalling Cisco Security Agent

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