



## CHAPTER 4

# Installing, Uninstalling, and Reinstalling Server Applications

This chapter describes the tasks that you must perform to install, uninstall, or reinstall Security Manager applications. It contains these major sections:

- [Installing Server Applications, page 4-1](#)
- [Uninstalling and Reinstalling Server Applications, page 4-6](#)



**Note**

The installation details in this chapter apply only if you are performing a fresh installation of Security Manager 3.2. If you are upgrading from an earlier version of Security Manager to 3.2, see [Chapter 5, “Upgrading and Downgrading Server Applications”](#).

## Installing Server Applications



**Tip**

To learn how to uninstall or reinstall Security Manager, see [Uninstalling and Reinstalling Server Applications, page 4-6](#).

You can install Security Manager 3.2 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 [Uninstalling and Reinstalling Server Applications, page 4-6](#).

### Before You Begin

- Read the [Readiness Checklist for Installation, page 3-4](#).
- For supported OS versions, see [Server Requirements, page 2-3](#).
- 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 3.2 requires that you use Common Services 3.1. Therefore, if you upgrade from an earlier Security Manager version, the installed Common Services version is also upgraded.
- Although Common Services enables you to configure Security Manager server to run in normal mode, we recommend that you enable browser-server security mode or SSL on your Security Manager server so that communication between the server and the client is secure.

- If you obtained a base license for Security Manager (see [Effects of Licensing on Installation, page 1-6](#)), 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** 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"> <li>• If autorun is enabled, the installer opens automatically.</li> <li>• If autorun is not enabled, open the <b>cs3m3_2_0_win_server</b> folder, double-click <b>Setup.exe</b>, and then click <b>Yes</b> to confirm that you are installing or upgrading Security Manager.</li> </ul> | <ul style="list-style-type: none"> <li>a. Go to <a href="http://www.cisco.com/go/csmanager">http://www.cisco.com/go/csmanager</a>, then click <b>Download Software</b>.</li> <li>b. Download <i>both</i> the documentation and the self-extracting software installation utility for Cisco Security Manager 3.2.</li> </ul> <p><b>Note</b> 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> <ul style="list-style-type: none"> <li>c. Print and read the documentation to learn what important considerations might affect your installation.</li> <li>d. Follow the instructions in the documentation for decompressing and starting the installation utility.</li> </ul> <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><b>Tip</b> 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 <a href="#">Changing the Default Location for Temporary Files, page C-3</a>.</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** Click **Next** in the Welcome screen of the wizard. The Software License Agreement screen is displayed.
- Step 3** Click **Yes** to agree to the License Agreement. If you decline the terms of the license, setup stops and installation does not occur. The installation program checks the name lookup and Dynamic Host Configuration Protocol (DHCP).
- Step 4** The Security Manager installer displays a warning if it detects any dynamic IP addresses on the target server. Click **Yes** to continue installation. Alternatively, click **No** to stop the setup, assign a static IP address and then restart the server.



**Note**

If the server has more than one IP address, you do not need to disable any of the multiple network interface cards before installation. Dynamic addresses are not supported.

**Step 5** The Backup Data screen is displayed only if you are not performing a fresh install of Security Manager on the server. Enter the full folder pathname in which to save the backup.

Alternatively, click **Browse** to navigate to a folder other than default. The Select Backup Folder dialog box is displayed.



---

**Note** If this screen appears, the backup is mandatory. You cannot complete the installation, reinstallation, or upgrade until you create a server backup.

---

**Step 6** From the hierarchical tree, select a folder in which to save the backup. If you want to choose a different drive from what is displayed, select a local drive from the drop-down list or click **Network** to select a volume on the network.

The full pathname of the selected folder in the Directories tree is displayed in the Path field. Click **OK** to continue.

**Step 7** The Choose Destination folder screen is displayed if you are performing a first-time installation or if Common Services is not already installed on your server. If you want to navigate to a folder other than the default, click **Browse** to make your selection and then click **OK** to confirm. Click **Next** to continue.



---

**Note** We recommend that you use the default folder location.

---

If a reinstallation fails because files remain in the folder that you use, you can manually back up and delete all such files, then delete all subfolders from the folder so that it is empty when you retry the reinstallation.

If you specify a folder other than the default folder, make sure that it does not contain any files and has fewer than 256 characters in its pathname.

---

**Step 8** If the folder you selected is not empty, an error message is displayed.

If you select Choose another folder to install Cisco Security Manager and click Next, setup returns to the Choose Destination Folder screen. Alternatively, if you select Use selected folder to install Cisco Security Manager and click Next, setup continues.

**Step 9** The Select Components screen is displayed. Select the check boxes next to the applications that you want to install on the server. Click **Next** to continue.



---

**Note** If you do not choose to install the client from this screen, you can download and install the client software installer later from the server home page.

---

If you want to run RME on a different server than the one in which you want to run Security Manager server, you need to select only Common Services in addition to RME from the component selection screen of the server installation wizard.

---

**Step 10** The System Requirements screen is displayed with the system requirements, available space in the drive and Temp Directory (%TEMP%), and available memory. Click **Next** to continue.

**Step 11** If you are installing Security Manager (rather than upgrading it), the Licensing Information screen is displayed.

Select one of the following:

- **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. If you have more than one license file, specify the base license. You can specify the permanent license file if you have previously staged it on the server.
- **Evaluation Only**—Enables the free 90-day evaluation period.




---

**Note** If you use the Professional Edition of Security Manager (see [Effects of Licensing on Installation, page 1-6](#)), see the Installing Security Manager License Files topic in the *User Guide for Cisco Security Manager 3.2* for information about installing any additional device license increments that you buy.

---

Click **Next** to continue. If you are not installing Common Services, go to [Step 12](#). Otherwise, the following screens are displayed to enable you configure the admin, System Identity, and casuser accounts.

- The Change Admin Password screen is displayed. Enter the password to associate with the admin username and confirm it. Click **Next** to continue.




---

**Note** The admin account can see everything in the Security Manager GUI and has full read/write privileges for all tasks and options.

---




---

**Tip** Passwords must be at least 5 characters long, but longer passwords are more secure.

---

- The Change System Identity Account Password screen is displayed. Enter a password to associate with the System Identity account username and confirm it. Click **Next** to continue the setup. Click **Yes** when prompted to confirm your creation of the System Identity account. If you are installing Common Services on the system for the first time, the Create casuser screen is displayed.




---

**Note** In a multi-server environment, you must configure all systems part of your multi-server setup with the same System Identity Account password.

The System Identity account can see everything in the Security Manager GUI and has full read/write privileges for all tasks and options.

---

- Click **No** to exit the installation and create casuser yourself and rerun the installation. Alternatively, click **Yes** to allow the installation program to create the local user casuser.




---

**Note** The casuser account can see everything in the Security Manager GUI and has full read/write privileges for all tasks and options.

---

**Step 12** The Summary screen is displayed, showing the summary of settings for the installation. If you want to view passwords and other security sensitive data, click **Show Details**.

If you click Show Details, the Security Alert dialog box appears.

- Click **Yes** in the Security Alert dialog box to view the Summary page with the passwords and other security sensitive data in cleartext. You can select and copy the data from the Summary page.

- Click **Hide Details** to hide the details.

Click **Next** to continue the setup. Click **Yes** when prompted to confirm your creation of the casuser account.



**Tip** After you click Next, an error message might tell you that files are running in another process and cannot be stopped automatically, but must be stopped before the installation can succeed. In this case, stop all applications, close all browsers, close all CLI prompts, then try again. If the message persists, restart the server and try again.

**Step 13** Click **Finish**.

Setup installs and configures the selected components.

**Step 14** 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 6, “Installing or Uninstalling Security Manager Client.”](#)
- Protected by the standalone version of Cisco Security Agent. See [Cisco Security Agent, page 1-5](#), and see [Appendix B, “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 C-4](#).



**Note** If you perform a fresh installation of Security manager 3.2 server, a bundle name might appear as “nu” with the version as “1.1” in the Bundles Installed table of the Software Updates page in the Common Services 3.1 GUI. You can ignore this entry as it does not refer to any valid bundle installed on your system.



**Caution**

If McAfee VirusScan is installed on your server *and* if you will install RME, 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. In addition, any RME 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.

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 1-7](#).

# 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 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 4-6](#)
- [Reinstalling Server Applications, page 4-8](#)

## Uninstalling Server Applications

This section describes how you can uninstall Security Manager and its related applications from your server. If you want to upgrade your server to Security Manager 3.2 from an earlier release using the backup and restore method, you must uninstall the previous release before installing 3.2 to restore the database.



## 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 B-3](#).

### 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 “Backing up and Restoring the Security Manager Database” section in the “Managing the Security Manager Server” chapter of the *User Guide for Security Manager 3.2*.
- 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 `\CSCOPx\bin` when you uninstall server applications, the uninstaller cannot delete `\CSCOPx\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 [Problems During Uninstallation, page A-5](#). For additional information about uninstallation error messages, see the “Troubleshooting and FAQs” chapter in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.0*: [http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_lan\\_management\\_solution/3.0/install/guide/IGSG.html](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/3.0/install/guide/IGSG.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, log in to your Cisco.com account and see “Impact of Installing CiscoWorks Applications in ACS Mode” in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.0*, at [http://www.cisco.com/en/US/docs/net\\_mgmt/cisoworks\\_lan\\_management\\_solution/3.0/install/guide/I\\_GSG.html](http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_lan_management_solution/3.0/install/guide/I_GSG.html).

---

- 
- 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 4-1](#).
-