



CHAPTER 6

Installing or Uninstalling Security Manager Client

You use Security Manager Client to manage security in your network through an encrypted connection to your Security Manager server, without regard to the physical location of your server.

The topics in this chapter are:

- [Client System Browser Best Practices, page 6-1](#)
- [Configuring Required Client Settings To Open Browser Windows, page 6-2](#)
- [Installing Security Manager Client, page 6-8](#)
- [Patching a Client, page 6-11](#)
- [Uninstalling Security Manager Client, page 6-12](#)
- [Using Security Manager Client To Log In to a Server, page 6-13](#)

Client System Browser Best Practices

Complete the following checklist to avoid problems with the client system browser that you use to:

- Download software installers from your server.
- Open certain applications on your server.

✓	Task
<input type="checkbox"/>	1. Make sure the browser cache is not set to zero. See your browser documentation for instructions.
<input type="checkbox"/>	2. Disable popup blockers. The method varies according to your installed popup blocker. See Configuring Required Client Settings To Open Browser Windows, page 6-2 , see your popup blocker documentation for more information, or contact the manufacturer for technical support.

Configuring Required Client Settings To Open Browser Windows

You must manage popup windows carefully on your client system when you access a Security Manager server, or some Security Manager product features might be unavailable to you—including the windows in which you configure server settings or view online help topics. You might have to change browser settings on a client system, and you might have to change settings in third-party utilities.

The topics in this section are our recommendations for managing browser settings and the settings for utilities that can affect popup windows on systems where you use Security Manager Client:

- [Configuring Internet Explorer Settings, page 6-2](#)
- [Configuring Firefox Settings, page 6-3](#)
- [Accessing Online Help Using Internet Explorer, page 6-5](#)
- [Enabling and Configuring Exceptions in Third-party Tools, page 6-8](#)

Configuring Internet Explorer Settings

[Table 6-1](#) describes the required Internet Explorer tasks for the different versions of Windows.

Table 6-1 *Internet Explorer Configuration Tasks on Client Systems*

Windows Server 2003, Windows XP, or Windows Vista	<p>You must allow active content, as follows:</p> <ol style="list-style-type: none"> 1. Select Tools > Internet Options, then click the Advanced tab. 2. Scroll to the Security section, then select Allow active content to run in files on My Computer. 3. Click OK.
	<p>Confirm if the browser security settings enable you to save encrypted pages to disk. If you cannot save encrypted pages, you cannot download the client software installer. To verify that you enabled the required setting, do the following:</p> <ol style="list-style-type: none"> 1. Select Tools > Internet Options, then click the Advanced tab. 2. Scroll to the Security area, then deselect the Do not save encrypted Pages to Disk check box. 3. Click OK.
	<p>Confirm that the size of the disk cache for temporary files is greater than the size of the client software installer that you expect to download. If the cache allocation is too small, you cannot download the installer. To change the cache size, do the following:</p> <ol style="list-style-type: none"> 1. Select Tools > Internet Options, then click Settings under the General tab. 2. Reserve more space for the cache if the setting is too small, then click OK twice. <p>We recommend that you manually delete the Temp files on your client system before you download the client software installer. Deleting such files increases the chances that you have enough available space.</p>

Configuring Firefox Settings

The following topics describe the Firefox configuration tasks required to display popup windows when you access the server from your Security Manager client or view the online help:

- [Editing the Preferences File](#), page 6-3
- [Editing the Size of the Disk Cache](#), page 6-3
- [Disabling the Popup Blocker or Creating a White List](#), page 6-3
- [Enabling JavaScript](#), page 6-4
- [Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests](#), page 6-4

Editing the Preferences File

To edit the preferences file, do the following:

-
- Step 1** From the \Mozilla Firefox\defaults\pref subdirectory, open **firefox.js** in a text editor, such as Notepad.
- Step 2** Add the following:
- ```
pref("dom.allow_scripts_to_close_windows", true);
```
- Step 3** Save, then close, the edited file.
- 

### Editing the Size of the Disk Cache

Confirm that the size of the disk cache for temporary files is greater than the size of the client software installer that you expect to download. If the cache allocation is too small, you cannot download the installer. To change the cache size, do the following:

- 
- Step 1** Select **Tools > Options**, then click **Advanced**.
- Step 2** Reserve more space for the cache if the setting is too small, then click **OK**.
- 

### Disabling the Popup Blocker or Creating a White List

To disable popup blockers, do the following:

- 
- Step 1** Select **Tools > Options**, then click the **Contents** icon.
- Step 2** Deselect the **Block pop-up windows** check box.

Alternatively, to create a white list of trustworthy sources from which to accept popups, select the **Block pop-up windows** check box, then click **Exceptions** and in the Allowed Sites - Popups dialog box:

- Enter **http://<SERVER\_NAME>** (where *SERVER\_NAME* is the IP address or DNS-routable name of your Security Manager server) in the Address of web site field, then click **Allow**.

- Enter **file:///C:/Documents%20and%20Settings/<USER\_NAME>/Local%20Settings/Temp/** (where *C*: is the client system disk drive on which you installed Windows and *USER\_NAME* is your Windows username on the client system), then click **Allow**.
- Click **Close**.

**Step 3** Click **OK**.

---

## Enabling JavaScript

To enable JavaScript, do the following:

**Step 1** Select **Tools > Options**, then click the **Contents** icon.

**Step 2** Select the **Enable JavaScript** check box.

**Step 3** Click **Advanced**, and in the Advanced JavaScript Settings dialog box, select every check box in the *Allow scripts to* area.

**Step 4** Click **OK**.

---

## Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests

When you access online help the first time, two new browser windows might be opened: a blank page and a page with help contents. Also, existing browser windows might not be reused during subsequent attempts to access online help. To configure Firefox to display online help on a new tab in the most recently opened browser window and to reuse existing windows on later occasions, follow these steps:

**Step 1** In the address bar, enter **about:config** and press **Enter**. The list of user preferences is displayed.

**Step 2** Double-click **browser.link.open\_external** and enter **3** in the resulting dialog box. This value denotes that links from an external application are opened in a new tab in the browser window that was last opened.

**Step 3** Double-click **browser.link.open\_newwindow** and set it to **1**. This value denotes that links are opened in the active tab or window.

**Step 4** Double-click **browser.link.open\_newwindow.restriction** and set it to **0**. This value causes all new windows to be opened as tabs.

**Step 5** Close the **about:config** page.



**Note** A blank page might be displayed when you open context-sensitive help, even after the browser status bar displays the status as Done. If this problem occurs, wait for a few minutes to allow the content to be downloaded and displayed.

---

**Note**

When you access online help for the first time, the Website Certified by an Unknown Authority dialog box might appear prompting you to examine and accept the certificate presented by Security Manager if it is not trusted by the browser. You can either accept the certificate for the remainder of the web browsing session or add the issuer identified in the certificate to the list of trusted CAs of the web browser and trust the certificate until it expires.

## Accessing Online Help Using Internet Explorer

If you are using Internet Explorer 6.0 or 7.0, online help does not load right away and you are prompted to respond to a series of warning or error messages before it can be displayed. These messages are displayed because of the default security settings of your browser. The following sections describe the actions to take when you access online help for the first time with default browser settings and to import the Security Manager certificate to the root certificate store in your browser:

- [Internet Explorer 6.0 Certificate Support for Online Help, page 6-5](#)
- [Internet Explorer 7.0 Certificate Support for Online Help, page 6-6](#)

### Internet Explorer 6.0 Certificate Support for Online Help

This procedure describes how to load online help for the first time. It also explains how to import the Security Manager certificate to the Internet Explorer 6.0 security store for secure access, without having to reload the certificate every time that you restart the browser.

**Note**

This procedure assumes that your browser is configured with default settings. If you cannot load the online help with the customized browser settings, you can restore them to their defaults and follow this procedure.

**Step 1** When you access online help from the application the first time, the following error message appears on the browser information bar:

```
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
```

**Step 2** To set the browser to allow blocked content, click the **here for options** link on the Internet Explorer information bar and choose **Allow Blocked Content**.

**Step 3** Select **Yes** when the Security Warning dialog box displays the following message. This message is not displayed if you already configured Internet Explorer to allow active content. See [Configuring Internet Explorer Settings, page 6-2](#) for more information.

```
Allowing active content such as script and ActiveX controls can be useful, but active content might also harm your computer. Are you sure you want to let this file run active content?
```

**Step 4** Another warning window appears stating that the security certificate is not fully valid and is not from a known source. Click **Yes** to accept the certificate presented by the Security Manager server.

Alternatively, click **View Certificate** to accept the certificate before proceeding. Go to [Step 7](#).

**Step 5** On some systems, a warning dialog box prompts you with the following message:

A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?

Click **Yes** to allow the page to continue downloading. This message is displayed because the default time that Internet Explorer waits before prompting the user to decide whether they want scripts that take excessive time to run. For more information on how to prevent this warning message from appearing, see the “Security Manager Client” chapter in the *FAQs and Troubleshooting Guide for Cisco Security Manager 3.2*.

The help page is displayed with the table of contents on the left pane and context-sensitive help on the right pane.

- Step 6** Double-click the lock icon on the status bar of the browser. The Certificate window is displayed with the General tab selected.
- Step 7** Click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears.
- Step 8** Click **Next**. The Certificate Store screen of the wizard appears, asking where you want to store the certificate.
- Step 9** By default, the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected. If you want to choose the location to store the certificate or if storing the certificate using the automatically selected folder option fails, click the **Place all certificates in the following store** radio button and click **Browse** to select the folder. Click **Next**. A window appears that states that you successfully imported the certificate.
- Step 10** Verify the setting and click **Finish**. A security warning displays for the import operation.
- Step 11** To install the certificate, click **Yes**. The Import Wizard displays “The import was successful.”
- Step 12** Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays “This certificate is OK.”
- Step 13** Click **OK** in the Certificate window, which is still displayed.
- Step 14** (Optional) If you viewed and accepted the certificate from the Security Alert dialog box, click **Yes** to close it.
- Step 15** To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the **Content** tab. Click **Certificates** and select the **Trusted Root Certifications Authorities** tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

## Internet Explorer 7.0 Certificate Support for Online Help

This procedure describes how to load online help for the first time. It also explains how to import the Security Manager certificate to the Internet Explorer 7.0 security store for secure access, without having to reload the certificate every time that you restart the browser.



### Note

This procedure assumes that your browser is configured with default settings. If you cannot load the online help with the customized browser settings, you can restore them to their defaults and follow this procedure.

- Step 1** When you access online help from the application, the following error message appears on the browser information bar:
- To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
- Step 2** To set the browser to allow blocked content, click the **here for options** link on the Internet Explorer information bar and choose **Allow Blocked Content**.
- Step 3** Select **Yes** when the Security Warning dialog box displays the following message. This message is not displayed if you already configured Internet Explorer to allow active content. See [Configuring Internet Explorer Settings, page 6-2](#) for more information.
- Allowing active content such as script and ActiveX controls can be useful, but active content might also harm your computer. Are you sure you want to let this file run active content?
- Step 4** The browser displays a Certificate Error: Navigation Blocked page to indicate this website is untrusted. To access the server, click **Continue to this website (not recommended)**. The browser displays the address bar and a Certificate Error status in red.
- Step 5** On some systems, a warning dialog box prompts you with the following message:
- A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?
- Click **Yes** to allow the page to continue downloading. This message is displayed because the default time that Internet Explorer waits before prompting the user to decide whether they want scripts that take excessive time to run. For more information on how to prevent this warning message from appearing, see the “Security Manager Client” chapter in the *FAQs and Troubleshooting Guide for Cisco Security Manager 3.2*.
- The help page is displayed with the table of contents on the left pane and context-sensitive help on the right pane.
- Step 6** Click the **Certificate Error** link at the top of the window. The Untrusted Certificate dialog box is displayed stating that the security certificate presented by this website was not issued by a trusted certificate authority.
- Step 7** Click **View Certificates**. The Certificate window is displayed with the General tab selected.
- Step 8** Click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears.
- Step 9** Click **Next**. The Certificate Store screen of the wizard appears, asking where you want to store the certificate.
- Step 10** By default, the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected. If you want to choose the location to store the certificate or if storing the certificate using the automatically selected folder option fails, click the **Place all certificates in the following store** radio button and click **Browse** to select the folder. Click **Next**. A window appears that states that you successfully imported the certificate.
- Step 11** Verify the setting and click **Finish**. A security warning displays for the import operation.
- Step 12** To install the certificate, click **Yes**. The Import Wizard displays “The import was successful.”
- Step 13** Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays “This certificate is OK.”
- Step 14** Click **OK** in the Certificate window, which is still displayed.

- Step 15** To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the **Content** tab. Click **Certificates** and select the **Trusted Root Certifications Authorities** tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

## Enabling and Configuring Exceptions in Third-party Tools

Some third-party popup blockers enable you to allow popups from a specific site or server without allowing popups universally. If your popup blocker does not allow you to configure exceptions to include in a white list, or if that option fails to meet your requirements, you must set your utility to allow all popups. The method for allowing popups from a trusted site varies according to the utility that you use. Please refer to the third-party product's documentation for more information.

## Installing Security Manager Client

You can install Security Manager Client during installation of Security Manager server by selecting the client software from the component selection screen of the server installation wizard. Otherwise, you can install the client software by logging in to the Security Manager server using a browser after you install the server software.

For supported OS versions on client systems, see [Client Requirements, page 2-5](#).

### Before You Begin

- (Windows XP) Select **Start > All Programs > Accessories > System Tools > System Restore**, then create a system restore point.
- (Windows 2003 or Windows XP) Internet Explorer Enhanced Security default settings might stop you from downloading the installation utility from your server. In this case, a message tells you that:

Internet Explorer cannot download CSMClientSetup.exe from <server>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.

To work around this problem, select **Start > Settings > Control Panel > Add or Remove Programs**, then click **Add/Remove Windows Components**. From the Windows Component Wizard window, deselect the **Internet Explorer Enhanced Security Configuration** check box, click **Next**, then click **Finish**.

- (Windows Vista) The system displays the User Account Control popup window to indicate that an unidentified program wants access to your computer. This occurs because of a limitation in the InstallAnywhere software. This one-time popup displays only when installing the client software. Select **Allow** to continue.
- (Windows XP SP2 and Vista) Increased security features might cause the following message to be displayed:

Security Warning Message. The publisher could not be verified. Are you sure you want to run this software?

When you see this message, click **Yes** to continue.

- (Windows Vista) When you download the client software from your server, a File Download - Security Warning dialog box appears asking, “Do you want to run or save this file?” Click **Save** to continue.
- Cisco Security Agent needs to be disabled, either before or during the process of installing the client. If the client installer is unable to disable the Cisco Security Agent during the installation process, the process aborts and you are prompted to manually disable it before restarting the client installation.
- 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.

**Note**

---

We recommend that you do not install both the Security Manager server software and Cisco Security Manager Client on the same system.

---

This procedure tells you how to install Security Manager Client without the server installer.

---

**Step 1** Log in to the client system from a user account that has Windows administrator privileges.

**Step 2** Use a browser on the client system to log in to the Security Manager server at:  
**http://<server\_name>:1741.**

To learn which browsers and browser versions are supported, see [Client Requirements, page 2-5](#).

**Step 3** After you log in, click **Cisco Security Manager Client Installer**.

**Step 4** Do one of the following. (The button names that your browser displays while you complete this step are determined by the browser, not by Security Manager.)

- **Open**—To run the installer from the server without downloading a local copy, click the correct button (most likely **Open**).
- **Save**—To save a local copy of the **CSMClientSetup.exe** file, click the correct button (most likely **Save**), then double-click the local file to start the installation.

The InstallAnywhere Wizard progress bar appears and prepares the system for installation. After a few seconds, the Introduction window appears.

**Tip**

---

If Cisco Security Agent is installed on the client system and opens the “A problem was detected” dialog box, select **Yes**, then click **Apply**. The dialog box closes, then the Installer window opens.

---

**Step 5** Click **Next**.

**Step 6** If Cisco Security Agent is installed and enabled on the client system, an error message is displayed that it must be disabled to proceed with the installation of the client software. Click **Yes** to disable the Cisco Security Agent. Alternatively, click **No** if you want to abort the installation and change the Cisco Security Agent settings yourself.

**Note**

---

If the client installer is unable to stop the Cisco Security Agent, an error message is displayed that the installation would be aborted and you need to manually disable it before restarting the installation.

---

**Step 7** (Optional) If a version of Security Manager client is already installed on the system, the wizard displays a message that the existing Security Manager client will be uninstalled. Click **Next** to continue.

A dialog box appears, indicating the uninstallation process, until the operation is complete. The Cisco Security Manager Server Information screen is then displayed.

**Step 8** Do all of the following, in any order:

- Specify the IP address or the DNS-resolvable hostname of a Security Manager server to which you will establish future connections.
- Ensure HTTPS is selected as the communications protocol. You cannot use HTTP.

**Step 9** Click **Next**. The Choose Shortcut Options screen is displayed.

**Step 10** Select one of the following options to configure the users for which a shortcut to the Security Manager client needs to be created:

- Create Shortcuts for Current User Only—Creates a desktop shortcut and a shortcut on the Programs menu only for the user who is currently installing the client software. This option is selected by default.




---

**Note** When you install Security Manager client as part of the server installation in silent mode, the shortcut to the client is created only for the user performing the installation by default.

---

- Create Desktop Shortcut for All Users—Creates a desktop shortcut and an option in the program listings in the Start menu for all user accounts configured on the system in which you are installing the client software. If the physical location of your client system is in the *network operations center* or *security operations center* for your organization, you might prefer to allow more than one Windows user to run the Security Manager Client application.
- Do Not Create Desktop Shortcut—Does not create a shortcut, either on the desktop or on the Programs menu for any user of the client system.

**Step 11** To specify the target directory for installation (the default is C:\Program Files\Cisco Systems\Cisco Security Manager Client), do one of the following in the Choose Installation Location screen:

- To use the default directory, click **Restore Default Folder** and click **Next**.
- To open a dialog box from which you can specify a different directory for installation, click **Browse**, then select a directory and click **Next**.

**Step 12** Review your selections, then click **Install** in the Pre-Installation Summary screen to confirm and proceed with the installation. In the event of an error, click **Back**, make any necessary corrections, then try again.

The Installing Cisco Security Manager Client screen appears with a dynamic indicator bar, which moves across the window. This bar indicates the progress of the installation process. When completed, a final screen displays indicating that the installation is completed.

**Step 13** Choose whether you want to start the Security Manager client after the installation is complete. Otherwise, you can start the client anytime after you complete the installation.

**Step 14** Click **Finish** to close the installer.




---

**Note** Apply the client software service pack or point patch, if you know that one is available. See [Patching a Client](#), page 6-11.

---

**Step 15** If you disabled an antivirus application temporarily, such as McAfee Antivirus or Norton Internet Security 2005, reenable it.

If the Cisco Security Agent was stopped by the client installer, it is restarted at the end of the installation. However if you manually disabled the Cisco Security Agent on your system, you need to enable it after client installation is complete.

**Step 16** (Optional) To start the client for Security Manager, do one of the following:

- If you let the installer create a desktop shortcut, double-click that shortcut.
- Select **Start > Programs > Cisco Security Manager > Cisco Security Manager Client**.



**Note**

If you changed the HTTP or HTTPS port number on your Security Manager server to a any port number other than the default value, connection to the server from the Security Manager client fails because the client tries to contact the server using the default port values. In Security Manager 3.2, two properties, HTTP\_PORT and HTTPS\_PORT, can be added to the client.info file located in the ..\Cisco Systems\Cisco Security Manager Client\jars folder on your client system to configure the port numbers you configured on your server. Add the following lines to the client.info file after opening it in a text editor such as Notepad and save the changes:

```
HTTP_PORT=<port_number>
HTTPS_PORT=<port_number>
```

When you start the client the next time, it uses the updated port numbers, based on the protocol selected, to communicate with the server.



**Tip**

If the Create Shortcuts for Current User Only option was selected during client installation, only the user who installs Security Manager Client can see (from the program listings in the Start menu) that the application is installed. Nonetheless, if the physical location of your client system is in the *network operations center* or *security operations center* for your organization, you might prefer to allow more than one Windows user to run the Security Manager Client application.

To make Security Manager Client visible in the Start menu for every user of the client station, copy the **Cisco Security Manager Client** folder from:

```
Documents and Settings\<user>\Start Menu\Programs\Cisco Security Manager to:
Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager.
```

## Patching a Client

After you apply a service pack or a point patch to your Security Manager server, each client system will prompt you to apply an update to your installed copies of Security Manager Client. The version number of the client software must be the same as the version number of the server software. When a client prompts you to download and apply a required software update, do the following.



**Note**

If the size of the disk cache for temporary files is lesser than the size of the client software update that you expect to download, see [Table 6-1 on page 6-2](#) for details on how to increase your disk cache space.

- 
- Step 1** Do one of the following. (The button names that your browser displays while you complete this step are determined by the browser, not by Security Manager.)
- If an error message says that the URL cannot be retrieved or that the connection timed out:
    - a. Uninstall the client software instead of patching it. See [Uninstalling Security Manager Client, page 6-12](#).
    - b. Download and install the new version of Security Manager Client. See [Installing Security Manager Client, page 6-8](#).
  - Open—To run the installer from the server without downloading a local copy, click the correct button (most likely *Open*).
  - Save—To save a local copy of the update installer, click the correct button (most likely *Save*), then double-click the local file to start the installation.

The InstallAnywhere Wizard prepares to install.

**Tip**

If Cisco Security Agent is installed on the client system and opens the “A problem was detected” dialog box, select **Yes**, then click **Apply**. The dialog box closes, then the Installer window opens.

---

- Step 2** When the update installer prompts you to specify an installation directory, specify the exact directory into which you installed Security Manager Client.

The default location is:

C:\Program Files\Cisco Systems\Cisco Security Manager Client.

- Step 3** If you are prompted to overwrite any existing files, click **Yes to All**.
- 

## Uninstalling Security Manager Client

If you installed Security Manager client on the same system as the Security Manager server software, you can uninstall the client using the server uninstaller. Alternatively, you can uninstall the client separately using the client uninstaller.

**Note**

When you install a Security Manager 3.2 client on a system in which a previous version of the client software exists, the installation wizard provides you with an option to uninstall the existing client before preparing the system for installing the 3.2 version.

---

This procedure tells you how to uninstall Security Manager Client outside of the server installation wizard.

---

- Step 1** Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager Client**. The InstallAnywhere Wizard prepares to uninstall, then the Uninstaller window opens.
- Step 2** To confirm that you have chosen to uninstall the client application, click **Next**.
- Step 3** Click **Finish**.

**Tip**

Even if the uninstaller does not prompt you specifically to restart your computer after you uninstall Security Manager Client, we recommend that you restart your computer.

## Using Security Manager Client To Log In to a Server

To connect to the Security Manager server from a system on which you have installed Security Manager Client:

- Step 1** Double-click the **Cisco Security Manager Client** icon on your Windows desktop or select **Start > Programs > Cisco Security Manager > Cisco Security Manager Client**.

**Note**

The Security Manager Client GUI appears after a short delay, during which no progress indicator is visible. The delay might last a few seconds.

- Step 2** Verify that your entries and selections are correct in the Cisco Security Manager Enterprise Edition window:
- **Server Name**—Contains the IP address or DNS-resolvable hostname of the server to which you will connect. You can edit the text to specify a different server or you can select an option from the list of server names.
  - **HTTPS** check box—Is required so that the server can use SSL to communicate with the client software. You must *not* deselect the HTTPS check box.
  - **User ID**—Contains the correct username for an account on the Security Manager server. To learn how to create a user account, see the Common Services documentation on Cisco.com.
  - **Password**—Contains the correct password for the account that you specified.
- Step 3** Click a button:
- To log in to the server with the specified credentials, click **Login**.
  - To exit the client without connecting to the server, click **Cancel**.
  - To understand how to log in, click **Help**.

**Note**

- If the server prompts you to download and install a client software update, see [Patching a Client, page 6-11](#).
- The client software automatically remembers the names of all servers to which you have logged in successfully. Each of those server names is added to the list of server names.

