



CHAPTER 5

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:

- [Configuring Required Client Settings To Open Browser Windows, page 5-1](#)
- [Installing Security Manager Client, page 5-5](#)
- [Patching a Client, page 5-10](#)
- [Uninstalling Security Manager Client, page 5-12](#)

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 5-2](#)
- [Configuring Mozilla Settings, page 5-3](#)
- [Enabling and Configuring Exceptions in Third-party Tools, page 5-4](#)

Configuring Internet Explorer Settings

The settings for Internet Explorer differ among the supported versions of Windows on your client systems. [Table 5-1](#) describes the required Internet Explorer tasks.

Table 5-1 *Internet Explorer Configuration Tasks on Client Systems*

Windows Server 2003 or Windows XP	<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.
Windows 2000	<p>You must allow JavaScript, as follows:</p> <ol style="list-style-type: none"> 1. Select Tools > Internet Options, click the Security tab, then click Custom Level. 2. Scroll to the Scripting section, then enable: <ul style="list-style-type: none"> • Active scripting. • Allow paste operations via script. • Scripting of Java applets. 3. Click OK.

Configuring Mozilla Settings

Table 5-2 describes the required Mozilla configuration tasks.

Table 5-2 *Mozilla Configuration Tasks on Client Systems*

Edit the preferences file.

1. From the \Mozilla\defaults\pref subdirectory, open **browser-prefs.js** in a text editor, such as Notepad.
2. Add the following:

```
pref("dom.allow_scripts_to_close_windows", true);
```
3. Save, then close, the edited file.

Disable the popup blocker or create a white list.

1. Select **Edit > Preferences**, then expand the **Privacy & Security** section in the Category pane.
2. Click **Popup Windows**, then deselect the **Block unrequested popup windows** check box.
Alternatively, to create a white list of trustworthy sources from which to accept popups, click **Popup Windows**, then click **Allowed Sites** and:
 - Enter **http://<SERVER_NAME>** (where *SERVER_NAME* is the IP address or DNS-routable name of your Security Manager server), then click **Add**.
 - 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 **Add**.
3. Click **OK** twice.

Enable JavaScript.

1. Select **Edit > Preferences**, then expand the **Advanced** section in the Category pane.
 2. Click **Scripts & Plug-ins**, then:
 - In the *Enable JavaScript for* area, select the **Navigator** check box.
 - In the *Allow scripts to* area, select every check box.
 3. Click **OK**.
-

Enabling and Configuring Exceptions in Third-party Tools

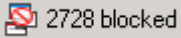
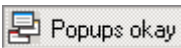
Some third-party popup blockers enable you to allow popups from a specific site or server without allowing popups universally. If your popup blocker does not allow you to configure exceptions to include in a white list, or if that option fails to meet your requirements, you must set your utility to allow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

If you use a popup blocker that has a configurable white list, you must do both of the following:

- Allow popup windows from the \Local Settings\Temp\ subdirectory that Windows associates with your Windows username on the client system. The path to that subdirectory might be, for example, C:\Documents and Settings*<username>*\Local Settings\Temp. Check the documentation for your popup blocker to learn whether it requires you to:
 - Use the **file://** protocol.
 - Use forward slashes (/) instead of back slashes (\) in Windows paths.
 - Replace any spaces in a pathname with this character string: %20.
- Allow popups from the Security Manager server, even if you block popups from all other servers.

Google Toolbar

As one example, you can allow popups from the Google Toolbar by clicking the **N blocked** button after you access a trusted server, so the button toggles to its **Popups okay** state.

	How the button looks by default. The number increases each time that Google Toolbar blocks a popup window.
	How the button looks when you allow popup windows from a site.

Google Toolbar adds the specified server to its white list and allows that server to open popup windows.

To allow *all* popups from Google Toolbar, select **Google > Options**, deselect the **Popup Blocker** check box, then click **OK**.

If you disable the popup-blocking feature in Google Toolbar—either universally or for a site that you add to your white list—but the utility continues to stop you from opening a window, you can hold down the **Ctrl** key while clicking a link that you know should open a popup window, to allow that one blocked window to open this one time.

Installing Security Manager Client



Caution

If you run an installation and an uninstallation *simultaneously* on the client system, even if they are for different applications, you corrupt the client system InstallShield database engine and are prevented from installing or uninstalling any software. For more information, log in to your Cisco.com account, then use Bug Toolkit to view [CSCsd21722](#) and [CSCsc91430](#).

For supported OS versions on client systems, see [Client Requirements, page 2-8](#).

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**.



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.

-
- Step 1** Log in to the client system from a user account that has Windows administrator privileges.
- Step 2** Disable antivirus applications temporarily, such as McAfee Antivirus or Norton Internet Security 2005.
- You cannot install Security Manager Client while antivirus programs are active.
- Step 3** If the client browser is Internet Explorer, confirm if its 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:
- Select **Tools > Internet Options**.
 - Click the **Advanced** tab.
 - Scroll to the Security area, then deselect the **Do not save encrypted Pages to Disk** check box.
 - Click **OK**.



Note Mozilla users do not have this problem, so there is no equivalent task in Mozilla.

- Step 4** 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.
- Internet Explorer—Select **Tools > Internet Options**, then click **Settings** under the General tab. Reserve more space for the cache if the setting is too small, then click **OK** twice.
 - Mozilla—Select **Edit > Preferences**, expand the **Advanced** list, then click **Cache**. Reserve more space for the cache if the setting is too small, then click **OK**.

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.

Step 5 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 2-8.

Step 6 After you log in, click **Cisco Security Manager Client Installer**.

Step 7 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 InstallShield Wizard prepares to install.

**Tip**

-
- If the client OS is Windows XP Professional (with SP2 applied) and a message warns you that the **CSMClientSetup.exe** software is unsigned, you can dismiss the warning. A known InstallShield bug prevents Cisco Systems from signing the installation utility.
 - 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.
-



Note Some buttons appear on more than one page in the installation wizard. You can use those recurring buttons as follows:

- **Back**—Click **Back** as many times as is necessary to return to an earlier prompt from which to change any unsatisfactory selections.
- **Next**—Click **Next** to confirm the selected values and advance to the next prompt.
- **Cancel**—Click **Cancel** to stop the installation.

Step 8 Click **Next**.

Step 9 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.
You might have to create an entry for your Security Manager server in the **hosts** file on your client system. Such an entry can help you to establish connections to your server if it is not registered with the DNS server for your network. To create this helpful entry on your client system, use **Notepad** or any other plain text editor to open **C:\WINDOWS\system32\drivers\etc\hosts**. (The host file itself contains detailed instructions for how to add an entry.)
- Specify the communications protocol to use. HTTPS is the default and is required. Do not select HTTP.



Note To understand communication protocol options on your Security Manager server, see the “Configuring the Server” chapter in *User Guide for CiscoWorks Common Services 3.0* on Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.0/user/guide/admin.html, or see that same section in the online help for Common Services.

- Confirm whether you want the installer to create a desktop shortcut.

Step 10 Click **Next**.

- 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:
- To use the default directory, 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 confirm or correct them.
- Step 13** In the event of an error, click **Back**, make any necessary corrections, then try again. Otherwise, wait for the Finish prompt.
- Step 14** Click **Finish**.
- Step 15** Apply the client software service pack or point patch, if you know that one is available. See [Patching a Client](#), page 5-10.
- Step 16** If you disabled an antivirus application temporarily, such as McAfee Antivirus or Norton Internet Security 2005, reenable it.
- Step 17** 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**.
-

**Tip**

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. See [Patching a Server, page 4-21](#). When a client prompts you to download and apply a required software update, do the following.

- Step 1** If the client browser is Internet Explorer, confirm if its security settings enable you to save encrypted pages to disk. If you cannot save encrypted pages, you cannot download the client software update installer. To verify that you enabled the required setting, do the following:
- a. Select **Tools > Internet Options**.
 - b. Click the **Advanced** tab.
 - c. Scroll to the Security area, then deselect the **Do not save encrypted Pages to Disk** check box.
 - d. Click **OK**.



Note Mozilla users do not have this problem, so there is no equivalent task in Mozilla.

- Step 2** Confirm that the size of the disk cache for temporary files is greater than the size of the client software update that you expect to download. If the cache allocation is too small, you cannot download the update.
- Internet Explorer—Select **Tools > Internet Options**, then click **Settings** under the General tab. Reserve more space for the cache if the setting is too small, then click **OK** twice.
 - Mozilla—Select **Edit > Preferences**, expand the **Advanced** list, then click **Cache**. Reserve more space for the cache if the setting is too small, then click **OK**.

We recommend that you manually delete the Temp files on your client system before you download the client update. Deleting such files increases the chances that you have enough available space.

**Caution**

If you run an installation and an uninstallation *simultaneously* on the client system, even if they are for different applications, you corrupt the client system InstallShield database engine and are prevented from installing or uninstalling any software. For more information, log in to your Cisco.com account, then use Bug Toolkit to view [CSCsd21722](#) and [CSCsc91430](#).

Step 3

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 5-12](#).
 - b. Download and install the new version of Security Manager Client. See [Installing Security Manager Client, page 5-5](#).
- 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 InstallShield Wizard prepares to install.

**Tip**

- If the client OS is Windows XP Professional (with SP2 applied) and a message warns you that the installation utility is unsigned, you can dismiss the warning. A known InstallShield bug prevents Cisco Systems from signing the installation utility.
- 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 4 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 5 If you are prompted to overwrite any existing files, click **Yes to All**.

Uninstalling Security Manager Client



Caution

If you run an installation and an uninstallation *simultaneously* on the client system, even if they are for different applications, you corrupt the client system InstallShield database engine and are prevented from installing or uninstalling any software. For more information, log in to your Cisco.com account, then use Bug Toolkit to view [CSCsd21722](#) and [CSCsc91430](#).



Note

Some buttons appear on more than one page in the uninstallation wizard. You can use those recurring buttons as follows:

- **Back**—Click **Back** as many times as is necessary to return to an earlier prompt from which to change any unsatisfactory selections.
 - **Next**—Click **Next** to confirm the selected values and advance to the next prompt.
 - **Cancel**—Click **Cancel** to stop the installation.
-

This procedure tells you how to uninstall Security Manager Client.

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

The InstallShield 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** Select the **Cisco Security Manager Client** check box if it is not already selected, then click **Next**.
- Step 4** Do one of the following:
- If the summary is correct, click **Next**.
 - If the summary is wrong, click **Back** so that you can correct your selections.
- Step 5** Click **Next**.

**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.
