CHAPTER 6

Installing and Configuring the Client

There are two main client applications that you use with Security Manager applications:

- The Security Manager client. This is a client-server application that is installed on your workstation and that interacts with the database running on the Security Manager server, which normally resides on another computer. This client also uses your web browser for some functions.
- A web browser. You use your web browser to use AUS and for configuring the Security Manager server and other servers that use Common Services.

The following topics describe how to configure your web browser to run the clients and how to install the Security Manager client:

Configuring Web Browser Clients

You must ensure that your web browser is configured to allow certain types of content and not to block popup windows from the server running the applications. The web browser is used for displaying online help as well as functional application windows. The following sections explain the browser settings you must configure so that you can use your browser effectively as an application client:

HTTP/HTTPS Proxy Exception

If you use an HTTP/HTTPS proxy, you need to configure a proxy exception for the Security Manager server.

This requirement applies to Internet Explorer and Firefox, for which additional configuration details are provided in the sections that follow.

Configuring Internet Explorer Settings

There are several settings that you need to configure in Internet Explorer for Security Manager and its applications to function correctly. Internet Explorer is used to display online help, activity reports, CS-MARS lookup information, and so forth. This procedure explains the settings you need to configure in Internet Explorer.

Procedure

Step 1 If you are using Internet Explorer 8, use Compatibility View; Internet Explorer 8 is supported only in Compatibility View. To use Compatibility View, open Internet Explorer 8, go to Tools > Compatibility View Settings, and add the Security Manager server as a "website to be displayed in Compatibility View."

Step 2 Turn off Pop-up Blocker for Security Manager by performing the following steps:

a. Open Internet Explorer

b. Go to Tools > Pop-up Blocker > Pop-up Blocker Settings

c. In the **Address of website to allow** field, enter the IP address of your Security Manager server and then click **Add**. Refer to http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions.

Caution If you do not turn off Pop-up Blocker, you may not be able to discover devices in Security Manager.

Tip "Pop-up Blocker is a feature in Internet Explorer that lets you limit or block most pop-ups." Refer to http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions.

Step 3 In Internet Explorer, select **Tools > Internet Options**. All subsequent steps in this procedure are performed on the Internet Options dialog box.

Step 4 Allow active content by performing the following steps:

a. Click the **Advanced** tab, scroll to the **Security** section, and select **Allow active content to run in files on My Computer**.

b. Click **Apply** to save your changes.

Step 5 Confirm that 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.

On the **Advanced** tab, in the Security area, deselect **Do not save encrypted Pages to Disk**. If you needed to change the setting, click **Apply** to save your changes.

Step 6 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. Change the cache size by performing the following steps:

a. Click the **General** tab.

b. Click **Settings** in the Temporary Internet Files group.

c. If necessary, increase the amount of disk space to use for temporary Internet files, and click **OK**.

d. Click **Apply** to save your changes.

Step 7 (Optional) Some interactions between CS-MARS and Security Manager require the opening of pages that have both secure and nonsecure content. By default, Internet Explorer asks you whether you want to display the nonsecure items. You can click **Yes** to this prompt and the software will function normally.

If desired, you can change the Internet Explorer settings so that you are not prompted and any page that has mixed content, that is, both secure and nonsecure content, are displayed automatically. Configure Internet Explorer to display mixed content pages by performing the following steps:

a. Click the **Security** tab.

b. Click **Custom Level** near the bottom of the dialog box.

c. Under the Miscellaneous heading, select the **Enable** radio button for the "Display mixed content" setting. (Ensure that you do not select Disable.)

d. Click **Apply** to save your changes.

Step 8 Click **OK** to close the Internet Options dialog box.

Configuring Firefox Settings

There are several settings that you need to configure in Firefox for Security Manager and its applications to function correctly. Firefox is used to display some features, such as online help, activity reports, CS-MARS lookup information, and so forth. This procedure explains the options you need to configure in Firefox.

- Editing the Preferences File, page 6-3
- Editing the Size of the Disk Cache, page 6-4
- Disabling the Popup Blocker or Creating a White List, page 6-4
- 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 6-5

Editing the Preferences File

Procedure

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, and 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.

Procedure

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

Procedure

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 do the following:

a. 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**.

b. 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**.

c. Click **Close**.

Step 3 Click **OK**.

Enabling JavaScript

Procedure

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.

Procedure

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.

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.

Tips for Installing the Security Manager Client

You use the Security Manager client to configure your devices. When you save changes in the client, they are saved to your workstation. You then must submit the changes to the database, which updates the database that resides on the server.

While using the client, there is constant back-and-forth communication between the client and the server. With that in mind, consider the following tips on installing the client to help improve client performance:

- Do not run the client on the same computer as the server as a normal day-to-day operation. If you install the client on the server, use it only for limited troubleshooting purposes.

- Install the client on workstations that are reasonably close to the server to avoid network latency problems. For example, if you have the server installed in the USA, a client running from a network in India might experience poor responsiveness due to the latency introduced. To alleviate this problem, you can employ a remote desktop or terminal server arrangement, where the clients are collocated in the same data center as the server.
- You can install only one copy of the client on a computer. There must be an exact version match between the client and server. Therefore, if you want to run two different versions of the Security Manager product, you must have two separate workstations for running the client.

  On the other hand, you can start the client multiple times to connect to different Security Manager servers that are running the same version.

Installing the Security Manager Client

The Security Manager client is a separate program that you install on your workstation. You use the client to log in to the Security Manager server and to configure security policies on your devices. The Security Manager client is the main application that you use with the product.

You might have already installed the client on the Security Manager server when you installed the server software. However, using the client on the same system as the server is not recommended for normal day-to-day usage of the product. Instead, you should install the client on a separate workstation using the following procedure. For information on workstation system requirements and supported browser versions, see Client Requirements, page 3-8.

If you run into problems during installation, see the following topics:

- Handling Security Settings That Prevent Installation, page 6-8
- Unable to Upgrade From a Previous Version of the Client, page 6-9
- Client Problems During Installation, page A-9.

Before You Begin

- Ensure that your browser is configured correctly. See Configuring Web Browser Clients, page 6-1.
- Ensure that Windows Firewall is configured correctly. On the operating systems supported by Security Manager, Windows Firewall is enabled by default. As a result, inbound connections for HTTP, HTTPS and syslog are blocked. For example, an admin can access the Security Manager client installation URL locally on the server but not from remote workstations. Another example is syslog data not showing up in Event Viewer. You must disable Windows Firewall or configure inbound rules to permit the management traffic in question.

Caution If you disable Windows Firewall on your workstation, it is vulnerable to malicious activity that Windows Firewall acts to prevent when it is enabled.

- 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.
- If it is installed on your workstation, the Cisco Security Agent needs to be disabled, either before or during the process of installing the client. If the client installer cannot 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.

Tip To disable Cisco Security Agent on your workstation, use one of the following two methods: (1) right-click the Cisco Security Agent icon in the system tray and select **Security Level > Off** or (2) open **Services** (Control Panel > Administrative Tools > Services), right-click **Cisco Security Agent**, and click **Stop**. After you finish installing the client, re-start Cisco Security Agent.

Caution While Cisco Security Agent is disabled on your workstation, it is vulnerable to malicious activity that Cisco Security Agent acts to prevent when it is enabled.

- If you already have the Security Manager client installed on the workstation, the installation program must uninstall it before installing the updated client. The wizard will prompt you if this is necessary.

Procedure

Step 1 Log in to the client workstation using a user account that has Windows administrator privileges.

Step 2 In your web browser, open one of these URLs, where SecManServer is the name of the computer where Security Manager is installed. Click **Yes** on any Security Alert windows.

- If you are not using SSL, open **http://***SecManServer***:1741**
- If you are using SSL, open **https://***SecManServer***:443**

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser.

Step 3 Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username **admin** and the password defined during product installation.

Step 4 On the Cisco Security Management Suite home page, click **Cisco Security Manager Client Installer**.

You are prompted to either open or run the file or to save it to disk. You can choose either option. If you choose to save it to disk, run the program after downloading it (double-click the file or select the Run option if your browser prompts you).

Tip If you get any security warnings about the application, such as "a problem was detected" or "the publisher cannot be verified" or that an unidentified application wants access to your computer, ensure that you allow the access. You might need to click more than one button, and the button names vary based on the application prompting you (such as Allow, Yes, Apply, and so forth).

Step 5 The installation wizard displays a "Welcome" screen with the following statement: Install these Cisco Security Manager 4.3 client applications:

- Configuration Manager
- Event Viewer
- Report Manager
- Health and Performance Manager
- Image Manager

The Security Manager client is installed as an application suite with five applications—Configuration Manager, Event Viewer, Report Manager, Health and Performance Manager, and Image Manager. Each can be launched independently in one of the following three ways (further information on launching the applications is available in Logging In To Security Manager Using the Security Manager Client, page 6-11):

- Start > Programs > Cisco Security Manager Client > [choose one of the following] Configuration Manager, Event Viewer, Report Manager, Health and Performance Manager, or Image Manager
- desktop icon
- [after starting one of the applications] Launch > [choose a different one of the applications in the Security Manager client application suite]

Note A desktop icon is also created for Cisco Security Manager. This icon opens the Cisco Security Management Suite home page.

Step 6 Follow the installation wizard instructions. During installation, you are asked for the following information:

- Server name—The DNS name or IP address of the server on which the Security Manager server software is installed. Normally, this is the server from which you downloaded the client installer.
- Protocol—HTTPS or HTTP. Select the protocol the Security Manager server is configured to use. Typically, the server is configured to use HTTPS. Ask your system administrator if you are not sure which to select. Also, if you know that the server is configured to use a non-default port, configure the port after installation using the information in Configuring a Non-Default HTTP or HTTPS Port, page 6-9.
- Shortcuts—Whether to create shortcuts for just yourself, for all user accounts that log in to this workstation, or for no users. This determines who will see Cisco Security Manager Client in the Start menu. You can start the client from Start > Programs > Cisco Security Manager Client > Cisco Security Manager Client or from the icon on the desktop.
- Installation location—The folder in which you want to install the client. Accept the default unless you have a compelling reason to install it elsewhere. The default location is C:\Program Files\Cisco Systems.

Step 7 Continue to follow the installation wizard instructions.

Step 8 After you click Done to complete the installation, if you disabled an antivirus application temporarily, re-enable it.

If the Cisco Security Agent on your workstation 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 must enable it after client installation is complete.

Handling Security Settings That Prevent Installation

There are many different ways you can configure security settings on your workstation, and many different products that you can install, that might prevent you from installing the Security Manager client. If you run into problems during installation, first ensure that your Windows user account has the administrative privileges required for installing software, then consider the following tips:

- (Windows XP) Internet Explorer Enhanced Security default settings might stop you from downloading the installation utility from your server. In this case, the following message appears:

  ```
  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**, and then click **Finish**.

- (Windows XP SP2) 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.

Configuring a Non-Default HTTP or HTTPS Port

The Security Manager server uses these default ports: HTTPS is 443; HTTP is 1741. If your organization installed the Security Manager server to use a different port, you need to configure the client to use the non-standard port. Otherwise, the client cannot connect to the server.

To configure different ports for your client, edit the **C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars\client.info** file using a text editor such as NotePad. Add the following settings and specify the custom port number in place of <*port number*>:

- HTTPS_PORT=<*port number*>
- HTTP_PORT=<*port number*>

These settings are used the next time you start the client.

Unable to Upgrade From a Previous Version of the Client

When you attempt to install the Security Manager client when you already have an older client installed, or when you used to have a client installed on the workstation, the client installer first uninstalls the previous version before installing the new one. If you receive the error message “Could not find main class. Program will exit,” the installer cannot install the client.

Procedure

This problem occurs because of the presence of old registry entries in your system. To correct this problem, do the following:

Step 1 Start the Registry Editor by selecting **Start > Run** and entering **regedit**.

Step 2 Remove the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\f427e21299b0dd254754c0d2778feec4-837992615

Step 3 Delete the previous installation directory, usually C:\Program Files\Cisco Systems\Cisco Security Manager Client.

Step 4 Rename the following folder:

C:\Program Files\Common Files\InstallShield\Universal\common\Gen1

Step 5 Select **Start > Control Panel > Add or Remove Programs**. If the Cisco Security Manager Client is still listed, click **Remove**. If you receive the message, "Program already removed; do you want to remove it from the list?", click **Yes**.

If you still cannot re-install the Security Manager client, rename the C:\Program Files\Common Files\InstallShield directory, then try again. Also see Client Problems During Installation, page A-9.

Patching a Client

After you apply a service pack or a point patch to your Security Manager server, the Security Manager client prompts you to apply an update when you log in to the server. The version number of the client software must be the same as the version number of the server software.

When you are prompted to download and apply a required software update, your web browser is used to download the update. You are prompted to either open or run the file, or to save it to disk. You can choose either option. If you choose to save it to disk, run the program after downloading it (double-click the file or select the Run option if your browser prompts you).

Installation of the patch is similar to installation of the client, and you must allow (or click **Yes**) to any security alerts from Cisco Security Agent or other security software you have installed to allow the installer to run.

When prompted for installation location, ensure that you select the folder in which you installed the client, and select **Yes to All** if you are asked if you want to overwrite files.

Tip If you get an error message that says that the URL cannot be retrieved or that the connection timed out, you need to uninstall the Security Manager client, then install a fresh copy (which will already have the patch applied). For more information, see Uninstalling Security Manager Client, page 6-13 and Installing the Security Manager Client, page 6-6.

Logging In to the Applications

After you have installed the server applications, configured your web browser, and installed the Security Manager client, you can log in to the applications:

- Logging In To Security Manager Using the Security Manager Client, page 6-11
- Logging In to Server Applications Using a Web Browser, page 6-12

Logging In To Security Manager Using the Security Manager Client

The Security Manager client is installed as an application suite with five applications—Configuration Manager, Event Viewer, and Report Manager. Each can be launched independently in one of the three ways described in the procedure below.

Use the Configuration Manager application (which is part of the Security Manager client application suite) to perform most Security Manager tasks.

Tip You must log in to the client workstation using a Windows user account that has Administrator privileges to fully use the Security Manager client. If you try to operate the client with lesser privileges, you might find that some features do not work correctly.

Procedure

Step 1 Launch your choice of Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, or Image Manager. Each can be launched independently in one of the following three ways:

- Start > Programs > Cisco Security Manager Client > [choose one of the following] Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, or Image Manager. The login dialog window appears.
- desktop icon. The login dialog window appears.
- [after starting one of the applications] Launch > [choose a different one of the applications in the Security Manager client application suite]. The login dialog window does not appear.

Step 2 In the Security Manager login dialog window, enter or select the DNS name of the server you want to log in to.

Note If you enter or select the IP address—instead of the DNS name—some features may not function as intended in an Internet Explorer 7 environment. To ensure the correct function of all Security Manager features, enter the DNS name of the server to which you want to log in.

Step 3 Enter your Security Manager username and password.

Step 4 If the server uses HTTPS for connections, ensure that the HTTPS check box is selected; otherwise, deselect it. Click **Login**.

Step 5 If the server prompts you to download and install a client software update, see Patching a Client, page 6-10.

Step 6 If there are no sessions running with the username and password that you just entered, the client application (Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, or Image Manager) logs in to the server and opens the client interface.

Step 7 If there is already a session running with the username and password that you just entered, an informational message appears to inform you that there is an easier way to launch the new application with the same session from the existing application. That way is the following:

[after starting one of the applications] Launch > [choose a different one of the applications in the Security Manager client application suite].

Step 8 The new application is launched from the existing session, or, if it is already running, it is brought to focus.

Tip The client closes if it is idle for 120 minutes. To change the idle timeout, select **Tools > Security Manager Administration**, select **Customize Desktop** from the table of contents, and enter the desired timeout period. You can also disable the feature so that the client does not close automatically.

Step 9 To exit Security Manager, select **File > Exit**.

Logging In to Server Applications Using a Web Browser

Only the Security Manager server uses a regular Windows application client for hosting the client application. All other applications, including the server administration features of Security Manager (through the Common Services application), CiscoWorks, and Auto Update Server are hosted in your web browser.

Logging in to these applications is identical. If you install more than one application on a single server, you log in to all installed applications at the same time. This is because the login is controlled by CiscoWorks, and all these applications are hosted under the CiscoWorks umbrella.

Procedure

Step 1 In your web browser, open one of these URLs, where *server* is the name of the computer where you installed any of the server applications. Click **Yes** on any Security Alert windows.

- If you are not using SSL, open http://*server*:1741.
- If you are using SSL, open https://*server*:443.

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser. For information on configuring the browser to run the applications, see Configuring Web Browser Clients, page 6-1.

Step 2 Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username **admin** and the password defined during product installation.

Step 3 On the Cisco Security Management Suite home page, you can access the features installed on the server. The home page can contain different items based on what you installed.

- Click the panel for the application that you want to run, such as **Auto Update Server**.
- Click the **Server Administration** panel to open the CiscoWorks Common Services Server menu. You can click this link to get to any place within Common Services. CiscoWorks Common Services is the foundation software that manages the server. Use it to configure and manage back-end server features such as server maintenance and troubleshooting, local user definition, and so on.
- Click the **CiscoWorks** link (in the upper right of the page) to open the CiscoWorks home page on the server.
- Click the **Cisco Security Manager Client Installer** to install the Security Manager client. The client is the main interface for using the Security Manager server.

Step 4 To exit the application, click **Logout** in the upper right corner of the screen. If you have both the home page and the Security Manager client open at the same time, exiting the browser connection does not exit the Security Manager client.

Uninstalling Security Manager Client

If you want to uninstall the Security Manager client, select **Start > Programs > Cisco Security Manager Client > Uninstall Cisco Security Manager Client** and follow the uninstallation wizard prompts.