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 must use your web browser 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, on page 1
- Tips for Installing the Security Manager Client, on page 5
- Installing the Security Manager Client, on page 5
- Logging In to the Applications, on page 10
- Uninstalling Security Manager Client, on page 12

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, on page 1
- Configuring Browser Cookies , on page 2
- Configuring Firefox Settings, on page 2
- Enabling and Configuring Exceptions in Third-party Tools, on page 5

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 Microsoft Edge and Firefox, for which additional configuration details are provided in the sections that follow.

Configuring Browser Cookies

When more than one browser is installed, the default browser's cookies should be enabled.

Blocking cookies can cause Security Manager user login to fail even after a clean installation of Security Manager. If user login fails after a clean installation of Security Manager, you may see the following error message: “CMF session id cannot be assigned.”

Configuring Microsoft Edge Settings

There are several settings that you need to configure in Microsoft Edge for Security Manager and its applications to function correctly. Microsoft Edge 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 Microsoft Edge.

Procedure

Procedure

Step 1 Turn off Pop-up Blocker for Security Manager by performing the following steps:

a) Open Microsoft Edge

b) Go to **Settings** > **Cookies and site permissions** > **Pop-ups and redirects**

c) In the **Allow** field, enter the IP address of your Security Manager server and then click **Add**. .

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

Step 2 If Jave script is not enabled by default on your Microsoft edge, do the following to enable it:

a) Select **Settings** > **Cookies and site permissions** > **JavaScript** > .

b) In the **Allow** field, click on the radio button to enable Java script.

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, on page 3
- Editing the Size of the Disk Cache, on page 3
- Disabling the Popup Blocker or Creating a White List, on page 3
- Enabling JavaScript, on page 4

• Displaying Online Help on a New Tab in the Most Recent Window and Reusing Existing Windows on Subsequent Requests, on page 4

Editing the Preferences File

Procedure

To edit the preferences file, do the following:

Procedure

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:

Procedure

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:

Procedure

Step 1 Select **Tools > Options**, then click the **Content** 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:

Procedure

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:

Procedure

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 for normal day-to-day operations. 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 more than once 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 3-11.

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

- Configuring a Non-Default HTTP or HTTPS Port, on page 8
- Unable to Upgrade From a Previous Version of the Client, on page 9
- Client Problems During Installation .

Before You Begin

- Ensure that your browser is configured correctly. See Configuring Web Browser Clients, on page 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**. For both of these two methods, you then need to take the following step for some versions of Windows: open **Services** right-click **Cisco Security Agent Monitor**, 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

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.

The Security Manager client is installed as a single application with six views—Configuration Manager, Event Viewer, Report Manager, Health and Performance Manager, Image Manager, and Dashboard. Each can be launched independently in one of the following three ways (further information is available in Logging In to Security Manager Using the Security Manager Client, on page 10):

- Start > All Programs > Cisco Security Manager Client [folder] > Cisco Security Manager Client
- [login screen]
- [after starting one of the views] Launch > [choose a different one of the views]

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, on page 8.

- 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 > All Programs > Cisco Security Manager Client [folder] > 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 (x86)\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.

From version 4.23, Cisco Security Manager lets you quietly install the Security Manager client in a background process, without having to spend a lot of time providing installation inputs, especially when installing on multiple servers.

- You can trigger the silent installation of the Security Manager client using a command in the following syntax: **CSMClientSetup.exe -i silent -DUSER_INSTALL_DIR=<Intended location for client to be installed>**. For example, the command can be **CSMClientSetup.exe -i silent -DUSER_INSTALL_DIR="C:\\Progra~2\\Ciso Systems\\Cisco Security Manager Client**.
- For uninstallation, use **Uninstall Cisco Security Manager Client*.exe -i silent**. For example, the command can be **C:\\Progra~2\\Ciso Systems\\Cisco Security Manager Client\\Uninstall_Cisco Security Manager Client\\Uninstall Cisco Security Manager Client 4.30.0.0.exe -i silent**.

Handling Security Settings That Prevent Installation

There are many different ways to configure security settings on your workstation, and many different products that you may have installed, 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 note:

Note If Microsoft Windows User Account Control (UAC) is turned on, you must install and run the client with "Run as administrator."

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 (x86)\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.

Change Port Utility

When required, you can change the web server port numbers for the Cisco Security Manager web server. You can also change both the HTTP and HTTPS port numbers, for which you will need administrative privileges. Run the following command at the prompt:

NMSROOT\MDC\Apache\changeport.exe

For example, you can enter **changeport 1744**, to change the Cisco Security Manager web server HTTP port to use 1744. You can alternatively use **changeport port number -s** to change the Security Manager web server HTTPS port to use the specified port number.

The follwing restrictions apply to the specified port number:

- Port numbers less than 1026 are not allowed. However, you can use 443 as the HTTPS port number.
- The specified port should not be used by any other service or daemon. The utility checks for active listening ports, and if any conflict is found, the utility rejects the specified port.
- There is no reliable way to determine whether any other service or application is using a specified port. If the service or application is running and actively listening on a port, it can be easily detected. However, if the service is currently stopped, there is no way that the utility can determine what port it uses. This is because on Windows there is no common port registry equivalent to /etc/services.

The port number must be a numeric value in the range 1026 - 65535. Values outside this range and other non-numeric values are not allowed.

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:

Procedure

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\{427e21299b0dd254754c0d2778feec4-837992615

Step 3 Delete the previous installation directory, usually C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client.

Step 4 Rename the following folder:

C:\Program Files (x86)\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 (x86)\Common Files\InstallShield directory, then try again. Also see Client Problems During Installation.

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 permit (or click **Yes**) 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, on page 12 and Installing the Security Manager Client, on page 5.

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, on page 10
- Logging In to Server Applications Using a Web Browser, on page 12

Logging In to Security Manager Using the Security Manager Client

The Security Manager client is installed as an application suite with six applications—Configuration Manager, Event Viewer, Report Manager, Health and Performance Monitor, Image Manager, and Dashboard. 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

Procedure

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

- Start > All Programs > Cisco Security Manager Client [folder] > Cisco Security Manager Client
- [login screen]
- [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.

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, on page 10.

Step 6 If you log in to a Security Manager server that is running a higher version than your client, a notification will be displayed and you will have the option of downloading the matching client version.

Step 7 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, Image Manager, or Dashboard) logs in to the server and opens the client interface.

Step 8 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 9 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 10 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), and CiscoWorks 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

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, on page 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 **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 **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 > All Programs > Cisco Security Manager Client > Uninstall Cisco Security Manager Client** and follow the uninstallation wizard prompts.