



## CHAPTER 2

# Security Manager Client

---

This chapter contains the following topics:

- [FAQs About the Security Manager Client, page 2-1](#)
- [Resetting the Client Password, page 2-2](#)
- [Using HTTP to Communicate with Server, page 2-3](#)
- [Display Problems in Dual-Screen Setup, page 2-3](#)
- [Wrong Message During Reinstallation of Client, page 2-5](#)
- [Unable to Upgrade From a Previous Version of Client, page 2-5](#)
- [Removing Another User's Locks in Non-Workflow Mode, page 2-6](#)
- [Loading the Online Help, page 2-6](#)
- [Preserving Search Results in Online Help, page 2-7](#)
- [Installation, Uninstallation, or Reinstallation, page 2-7](#)
- [Unable to Display Activity Report, page 2-7](#)



### Note

For detailed information on installing and uninstalling the Security Manager Client, see the “Installing or Uninstalling Security Manager Client” chapter in the [installation guide for Cisco Security Manager](#) for your release.

---

## FAQs About the Security Manager Client

This section answers the following questions about the Security Manager client:

- [Q.Can I install the Security Manager client on the same machine as the Security Manager server?](#)
- [Q.How can I clean up the server list from the Server Name field in the Login window?](#)
- [Q.What do I do if I forget to enter the server name during installation?](#)
- [Q.The Security Manager client GUI did not load because of a version mismatch. What does this mean?](#)
- [Q.Where are the client log files located?](#)
- [Q.How do I know if Security Manager is running in HTTPS mode?](#)

- Q.** Can I install the Security Manager client on the same machine as the Security Manager server?
- A.** We recommend that you do *not* install both the Security Manager server software and Cisco Security Manager client on the same system. However, if you do install it on the same system, if the Cisco Security Agent asks if you want to allow a process to start, you must allow it or the Security Manager client might behave erratically and stop working.
- Q.** How can I clean up the server list from the Server Name field in the Login window?
- A.** Delete `csmsserver.txt` from the directory in which you installed the Security Manager client. The default location is `C:\Program Files\Cisco Systems\Cisco Security Manager Client`.
- Q.** What do I do if I forget to enter the server name during installation?
- A.** In the Server Name field in the Login window, enter the server name. Names of servers that you successfully logged in to are remembered and appear in the list the next time you login.
- Q.** The Security Manager client GUI did not load because of a version mismatch. What does this mean?
- A.** The Security Manager server version does not match the client version. To fix this, download and install the most recent client installer from the server.
- Q.** Where are the client log files located?
- A.** The client log files are located in `C:\Program Files\Cisco Systems\Cisco Security Manager Client\logs`. Each GUI session has its own log file.
- Q.** How do I know if Security Manager is running in HTTPS mode?
- A.** Do one of the following:
- Look at the HTTPS check box in the Login window. If it is selected, Security Manager is running in HTTPS mode.
  - After you log in, look at the URL in the address field. If the URL starts with `https`, Security Manager is running in HTTPS mode.
  - Go to **Common Services > Server > Security > Single Server Management > Browser-Server Security Mode Setup**. If you see **Current Setting: Enabled**, Security Manager is running in HTTPS mode.
- Q.** How can I enable the Client Debug log level?
- A.** In the file `client.info`, which is located by default in `C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars`, modify the `DEBUG_LEVEL` parameters to include `DEBUG_LEVEL=ALL` and then restart the Security Manager client.

## Resetting the Client Password

If you cannot remember the password to the Security Manager client that was entered during installation, an administrator can reset the password using this procedure.



### Caution

This procedure does not require knowledge of the old password; therefore, it is important to keep the Security Manager server physically secure from unauthorized users.

- 
- Step 1** On the Security Manager server, shut down the Cisco Security Manager Daemon Manager service.
  - Step 2** Navigate to *NMSROOT*\bin. The default value for this location is C:\Program Files\CSCOp\bin.
  - Step 3** Open a command line and enter the command: `resetpasswd [username]`.
  - Step 4** At the prompt, enter and confirm new password. Passwords can range from 5 to 256 characters in length and can include any printable character.
  - Step 5** Restart the Daemon Manager.
- 

## Using HTTP to Communicate with Server

**Problem** You want the Security Manager client to use HTTP to communicate with the Security Manager server, instead of HTTPS.

**Solution** Do the following:

- 
- Step 1** In a web browser, enter `http://[Security_Manager_server]:1741`. This launches the web interface for the Security Manager server.
  - Step 2** Log in as an administrator, then click the **CiscoWorks** link in the upper-right corner.
  - Step 3** Under Common Services, select **Server > Security > Single-Server Management > Browser-Server Security Mode Setup**.
  - Step 4** Change the setting from Enable to Disable.
  - Step 5** Click **Apply**.
  - Step 6** Restart the Security Manager server.
  - Step 7** When you start the Security Manager client, be sure to deselect the **HTTPS** check box on the login screen.
- 



**Note** For security reasons, we recommend that you use HTTPS instead of HTTP.

---

## Display Problems in Dual-Screen Setup

**Problem** When working with a dual-screen setup, certain windows and popup messages always appear on the primary screen, even when the Security Manager client is running on the secondary screen. For example, with the client running on the secondary screen, windows such as the Policy Object Manager always open in the primary screen.

**Solution** This is a known issue with the way dual-screen support is implemented in certain operating systems. We recommend running the Security Manager client on the primary screen. You should launch the client after configuring the dual-screen setup.

**Tip**

---

If a window opens on the other screen, you can move it by pressing Alt+spacebar, followed by M; you can then use the arrow keys to move the window.

---

## Wrong Message During Reinstallation of Client

**Problem** When you attempt to install the Security Manager client (or perform a reinstall, for example, after upgrading the operating system), the installer displays a message stating that a previous version of the client is installed on your system and that it will be uninstalled.

**Solution** During installation or reinstallation of the client, the installer might detect a previously installed client, even if no such client exists, and display an incorrect message that it will be uninstalled. This message is displayed because of the presence of certain old registry entries in your system. Although client installation proceeds normally when this message appears, do the following to delete old registry entries and prevent this message from being displayed during subsequent installations:

- 
- Step 1** At the command line, type `regedit`, then press **Enter** to open the Registry Editor.
  - Step 2** Remove the following registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client
  - Step 3** Delete the previous installation directory.
  - Step 4** Navigate to the `..\Program Files\Zero G Registry` folder and rename the “.com.zerog.registry.xml” file located under this folder.
- 

## Unable to Upgrade From a Previous Version of Client

**Problem** When you attempt to install the Security Manager client (or perform an upgrade from a previous version to 3.3), you receive the “Could not find main class. Program will exit.” error message.

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

- 
- Step 1** At the command line, type `regedit`, then press **Enter** to open the Registry Editor.
  - Step 2** Remove the following registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{427e21299b0dd254754c0d2778feec4-837992615}
  - Step 3** Delete the previous installation directory.
  - 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**.

**Note**

If you are still unable to reinstall the Security Manager client, rename the C:\Program Files\Common Files\InstallShield directory, then try again.

After you complete the preceding steps, no error message is displayed when you retry the installation or upgrade operation.

## Removing Another User's Locks in Non-Workflow Mode

**Problem** When working in non-workflow mode, you discover that certain devices and policies that you need to configure are locked by another user. The locks remain in place until the other user submits or discards the configuration changes.

**Solution** If you have administrative permissions, you can remove the locks placed by another user by taking over that user's session. Select **Tools > Security Manager Administration > Take Over User Session**, then select the session. You can then submit or discard the user's changes to remove the locks.

## Loading the Online Help

**Problem** You cannot load the online help.

**Solution**

When using Internet Explorer as your default browser, try the following:

- Windows Server 2003, Windows XP, or Windows Vista—Select **Tools > Internet Options > Advanced > Security > Allow active content to run in files on My Computer**.
- When you access online help the first time using Internet Explorer 6.0 or 7.0, the page does not load right away and you are prompted 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. For detailed instructions on 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, see the “Installing or Uninstalling Security Manager Client” chapter in the *Installation Guide for Cisco Security Manager 3.3*.

When using Firefox as your default browser, try the following:

- Add the following line to open \Mozilla Firefox\defaults\pref\firefox.js:
 

```
pref("dom.allow_scripts_to_close_windows", true);
```
- Enable Javascript.
- 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, see the “Installing or Uninstalling Security Manager Client” chapter in the *Installation Guide for Cisco Security Manager 3.3*.

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.

## Preserving Search Results in Online Help

**Problem** When you click the link for one of the topics displayed in the online help search results, clicking the Search tab again (for example, to try a different topic listed in the search results) erases the results.

**Solution** Use the Back button in the browser instead of clicking the Search tab. The results of the previous search will still be displayed.

## Unable to Display Activity Report

**Problem** If you are using Internet Explorer as your default browser, Activity Change Report in PDF does not appear when you click View Changes from the Tools menu (nonWorkflow mode), or Activity Manager (Workflow mode).

**Solution** This problem occurs because of inaccuracies with the location of some of the dll files or invalid registry key values associated with Internet Explorer. For information on how to work around this problem, refer to the Microsoft Knowledge Base article 281679, which is available at this URL: <http://support.microsoft.com/kb/281679/EN-US>.

## Installation, Uninstallation, or Reinstallation

See the [installation guide for Cisco Security Manager](#) for your release for information about troubleshooting problems that are related to the installation, uninstallation, or reinstallation of:

- Security Manager (including Common Services) software on a server.
- Security Manager Client.
- The standalone version of Cisco Security Agent that is installed on most Security Manager servers.

For information regarding the installation of the Security Manager License, see *Cisco Security Manager 3.x: Steps to Install the License for Various Options* on Cisco.com at:

[http://www.cisco.com/en/US/products/ps6498/products\\_tech\\_note09186a0080849150.shtml](http://www.cisco.com/en/US/products/ps6498/products_tech_note09186a0080849150.shtml)

