



APPENDIX **A**

Troubleshooting

CiscoWorks Common Services 3.2 provides Security Manager with its framework for installation, uninstallation, and reinstallation on servers. If the installation or uninstallation of Security Manager server software causes an error, see “Troubleshooting and FAQs” in the Common Services online help or read it on Cisco.com:

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/I GSG31.html

These topics help you to troubleshoot problems that might occur when you install, uninstall, or reinstall Security Manager-related software applications on a client system or on a server, including the standalone version of Cisco Security Agent.

- [Questions and Answers, page A-1](#)
- [Troubleshooting the Standalone Security Agent, page A-12](#)
- [Running a Server Self-Test, page A-13](#)
- [Collecting Server Troubleshooting Information, page A-14](#)
- [Viewing and Changing Server Process Status, page A-14](#)
- [Reviewing the Server Installation Log File, page A-15](#)

Questions and Answers

Topics in this section answer questions that you might ask about installing, uninstalling, or reinstalling Security Manager and IPS Event Viewer successfully:

- [Note About Cisco Security Manager Services, page A-1](#)
- [Server Q&A, page A-2](#)
- [IPS Event Viewer Q&A, page A-7](#)
- [Client Q&A, page A-7](#)

Note About Cisco Security Manager Services

Cisco Security Manager services must be started in a specific order for Security Manager to function correctly. The initialization of these services is controlled by the Cisco Security Manager Daemon Manager service. You should not change the service startup type for any of the Cisco Security Manager

services. You should also not stop or start any of the Cisco Security Manager services manually. If you need to restart a specific service, you should restart the Cisco Security Manager Daemon Manager which will ensure that all the related services are stopped and started in the correct order.

Server Q&A

This section answers questions that you might have about:

- [Problems During Installation, page A-2](#)
- [Problems After Installation, page A-4](#)
- [Problems During Uninstallation, page A-5](#)

Problems During Installation

- Q.** When I install the server software, what does this installation error message mean?
- A.** Server software installation error messages and explanations appear in [Table A-1 on page A-2](#), where they are sorted alphabetically by their first word.

Table A-1 **Installation Error Messages (Server)**

| Message | Reason for Message | User Action |
|--|---|--|
| License file failed. ERROR: The file with the name c:\progra-1\CSCOpX\setup does not exist | An earlier attempt to uninstall a Common Services-dependent application failed. | <ol style="list-style-type: none"> 1. Shut down the server, then restart it. 2. Use a Registry editor to delete this entry: \$HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager\CurrentVersion. 3. In the directory where you installed Security Manager, create a subdirectory named <i>setup</i>. 4. If it exists, delete the CMFLOCK.TXT file. 5. Reinstall Security Manager. |
| Corrupt License file. Please enter a valid License file. | Your license file is corrupted or the contents of the license file are invalid. | See Getting Help with Licensing, page 1-6 . |
| Corrupt License file entered for 5 tries. Install will proceed in EVAL mode. Press OK to proceed. | You entered the pathname to an invalid license file for five consecutive attempts. After five failed attempts, installation continues in evaluation mode. | Click OK to close the license error dialog box, and installation proceeds to the next screen of the wizard. |
| One instance of CiscoWorks Installation is already running. If you are sure that no other instances are running, remove the file C:\CMFLOCK.TXT. This installation will now abort. | An earlier attempt to install a Common Services-dependant application failed. | Delete the C:\CMFLOCK.TXT file, then try again. |

Table A-1 Installation Error Messages (Server) (continued)

| Message | Reason for Message | User Action |
|--|---|--|
| Severe Failed on call to FileInsertLine. | Your server does not meet the requirement for hard drive space. | See Server Requirements, page 2-4 . |
| Temporary directory used by installation has reached _istmp9x. If _istmp99 is reached, no more setups can be run on this computer, they fail with error -112. | Temporary files that are supposed to be deleted automatically during software installations have not been deleted on your server. | Search the temporary directory on your server for subdirectories with names that include the “_istmp” string. Delete all such subdirectories. |
| Windows cannot find 'C:\Documents and Settings\Administrator\WINDOWS\System32\cmd.exe'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search. | You left Terminal Services enabled during installation, even though we do not support this. See Readiness Checklist for Installation, page 3-4 . | <ol style="list-style-type: none"> 1. Disable Terminal Services. To learn how to do this, see the “Terminal Server Support for Windows 2000 and Windows 2003 Server” topic in <i>Installing and Getting Started With CiscoWorks LAN Management Solution 3.1</i>, at http://www.cisco.com/en/US/docs/net_mgmt/cisco_works_lan_management_solution/3.1/install/guide/IGSG31.html 2. Try again to install Security Manager. |
| Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432. | The installation program checks the Windows account permissions during installation. If the Windows account that you are installing CiscoWorks Common Services under does not have local administrator privileges, InstallShield displays this error message. | <ol style="list-style-type: none"> 1. Verify that you have appropriate permissions to write to %WINDIR%. Installation or uninstallation has to be done by a member of local administrators group. 2. Click OK to close the error message, log out of Windows, and log back into Windows using an account that has local administrator privileges. |

Note For additional information about installation error messages, see the Common Services 3.2 documentation on Cisco.com.

- Q.** What should I do if the server installer suspends operation (hangs)?
- A.** Reboot and try again.
- Q.** Can I install both Cisco Security Manager and Cisco Secure Access Control Server on one system?
- A.** We recommend that you do not. We do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.
- Q.** Can Security Manager 3.3 coexist on a server with any older version of Common Services than 3.2?
- A.** We do not support coexistence on the same server with any Common Services version older than 3.2.

See <http://www.cisco.com/go/csmanager> for announcements of any new features or supported configurations.

Problems After Installation

- Q.** The Security Manager GUI does not appear, or is not displayed correctly, or certain GUI elements are missing. What happened?
- A.** There are several possible explanations. Investigate the scenarios in this list to understand and work around simple problems that might affect the GUI:
- Some required services are not running on your server. Restart the server daemon manager, wait for all services to start completely, then restart Security Manager Client and try again to connect.
 - Your server does not have enough free disk space. Confirm that the Security Manager partition on your server has at least 500 MB free.
 - Your base license file is corrupted. See [Getting Help with Licensing, page 1-6](#).
 - Your server uses the wrong Windows language. Only English, on US-English versions of Windows, and Japanese, on Japanese versions of Windows, are supported. (See [Server Requirements, page 2-4](#).) Any other language can corrupt the installed version of Security Manager, and missing GUI elements are one possible symptom. If you are using an unsupported language, you must select a supported language, then uninstall and reinstall Security Manager. See [Uninstalling and Reinstalling Server Applications, page 4-5](#).
 - Problems occurred when you installed Cisco Security Agent. You can check its installation log to learn whether problems interfered with the installation. See [Troubleshooting the Standalone Security Agent, page A-12](#).
 - You ran the Security Manager installation utility over a network connection, but we do not support this use case (see [Installing Server Applications, page 4-1](#)). You must uninstall and reinstall the server software. See:
 - [Uninstalling Server Applications, page 4-6](#).
 - [Reinstalling Server Applications, page 4-7](#).
 - Your client system does not meet the minimum requirements. See [Client Requirements, page 2-6](#).
 - You tried to use HTTP, but the required protocol is HTTPS.
 - Buttons are the only missing element. You opened the Display Properties control panel on the client system, then changed one or more settings under the Appearance tab while you were simultaneously using Security Manager Client. To work around this problem, exit Security Manager Client, then restart it.
 - The wrong graphics card driver software is installed on your client system. See [Client Requirements, page 2-6](#).
- Q.** Security Manager sees only the local volumes, not the mapped drives, when I use it to browse directories on my server. Why?
- A.** Microsoft includes this feature by design in Windows, to enhance server security. For more information, log in to your Cisco.com account, then use Bug Toolkit to learn about [CSCsb43414](#).



Note You must store your Security Manager license files on a volume that is local to your server, due to the restricted browsing of mapped drives.

- Q.** Why is Security Manager missing from the Start menu in my Japanese version of Windows?

- A.** You might have configured the regional and language option settings on the server to use English. We do not support English as the language in any Japanese version of Windows (see [Server Requirements, page 2-4](#)). Use the Control Panel to reset the language to Japanese.
- Q.** My server SSL certificate is no longer valid. Also, the DCRServer process does not start. What happened?
- A.** You reset the server date or time so that it is outside the range in which your SSL certificate is valid. See [Readiness Checklist for Installation, page 3-4](#). To work around this problem, reset the server date/time settings.
- Q.** I was not prompted for the protocol to be used for communication between the server and client. Which protocol is used by default? Do I need to configure this setting manually using any other mode?
- A.** HTTPS is used as the communication protocol between the server and client, by default, when you install the client in silent mode during the server installation. Because the communication is secure with the default protocol, you might not need to modify this setting manually.

An option to select HTTP as the protocol is available only when you run the client installer to install Security Manager client separately outside of the server installer. However, we recommend that you do not use HTTP as the communication protocol between the server and client.

Problems During Uninstallation

- Q.** What does this uninstallation error message mean?
- A.** Uninstallation error messages and explanations appear in [Table A-2 on page A-5](#), where they are sorted alphabetically by their first word.

Table A-2 Uninstallation Error Messages

| Message | Reason for Message | User Action |
|--|---|--|
| C:\NMSROOT\MDC\msfc-backend refers to a location that is unavailable. It could be on a hard drive on this computer, or on a network. Check to make sure that the disk is properly inserted, or that you are connected to the Internet or your network, and then try again. If it still cannot be located, the information might have been moved to a different location. | The message might be benign, and clicking OK to dismiss it might be all that is required. Otherwise, the message might appear on servers where either or both of the following conditions apply: - Simple file sharing is enabled in Windows. - Offline file synchronization is enabled in Windows. | If you dismiss the message and the uninstallation fails, try either or both of these possible workarounds, then try again to uninstall: Simple File Sharing <ol style="list-style-type: none"> 1. Select Start > Settings > Control Panel > Folder Options. 2. Click the View tab. 3. Scroll to the bottom of the Advanced Settings pane. 4. Deselect the Use simple file sharing (Recommended) check box, then click OK. Offline File Synchronization <ol style="list-style-type: none"> 1. Select Start > Settings > Control Panel > Folder Options. 2. Click the Offline Files tab. 3. Deselect the Enable Offline Files check box, then click OK. |

Table A-2 Uninstallation Error Messages (continued)

| Message | Reason for Message | User Action |
|--|---|--|
| <p>C:\temp\<i><subdirectory></i>\ setup.exe - Access is denied.</p> <p>The process cannot access the file because it is being used by another process.</p> <p>0 file(s) copied. 1 file(s) copied.</p> | Uninstallation failed. | Reboot the server, then complete the procedure described in Uninstalling Server Applications, page 4-6 . |
| <p>Windows Management Instrumentation (WMI) is running.</p> <p>The setup program has detected Windows Management Instrumentation (WMI) services running. This will lock some Cisco Security Manager processes and may abort uninstallation abruptly. To avoid this, uninstallation will stop and start the WMI services.</p> <p>Do you want to proceed?</p> <p>Click Yes to proceed with this uninstallation. Click No to exit uninstallation.</p> | Either your organization uses WMI or someone enabled the WMI service accidentally on your server. | Click Yes . |

Note For additional information about uninstallation error messages, see the Common Services 3.2 documentation on Cisco.com.

- Q.** What should I do if the uninstaller hangs?
- A.** Reboot, then try again.
- Q.** What should I do if the uninstaller displays a message to say that the *crmdmgt* service is not responding and asks “Do you want to keep waiting?”
- A.** The uninstallation script includes an instruction to stop the *crmdmgt* service, which did not respond to that instruction before the script timed out. Click **Yes**. In most cases, the *crmdmgt* service then stops as expected.

IPS Event Viewer Q&A

- Q.** How can I confirm if IPS Event Viewer installed correctly on my server when I installed Security Manager?
- A.** Log in as a Windows administrator on your Security Manager server, then do the following:
1. From the *NMSROOT\IEV\log* subdirectory, open **system.log**—where *NMSROOT* is the directory in which you installed Common Services (C:\Program Files\CSCOpX, for example). The logfile should contain exactly this text, and nothing else:
`Cisco IPS Event Viewer service successfully started.`
 2. Select **Start > Settings > Control Panel > Administrative Tools > Services**, then confirm that the following Windows services have started:
 - Cisco IPS Event Viewer
 - MySQL
- Q.** Does the Windows service called “Cisco IPS Event Viewer” have any special dependencies?
- A.** Yes. It cannot run successfully unless the Windows service called “MySQL” is also running.
- Q.** Can I uninstall IPS Event Viewer separately from Security Manager on my server?
- A.** If you used the Security Manager installer to install IPS Event Viewer, you cannot uninstall IPS Event Viewer without uninstalling Security Manager at the same time. Although IPS Event Viewer is displayed in the list of installed programs in the Add/Remove Programs window after installation, we recommend that you uninstall IPS Event Viewer using the Security Manager uninstaller instead of using the Add/Remove Programs control panel.

Client Q&A

This section answers questions that you might have about:

- [Problems During Installation, page A-7](#)
- [Problems After Installation, page A-10](#)
- [Other Problems, page A-11](#)

Problems During Installation

- Q.** When I install the client software, what does this installation error message mean?
- A.** Client software installation error messages and explanations appear in [Table A-3](#), where they are sorted alphabetically by their first word.

Table A-3 Installation Error Messages (Client)

| Message | Reason for Message | User Action |
|--|--|---|
| Could not install engine jar | Previous software installations and uninstallations caused InstallShield to run incorrectly. | <ol style="list-style-type: none"> 1. Navigate to: C:\Program Files\ Common Files\ InstallShield\Universal\ common\Gen1. 2. Rename the Gen1 folder, then try again to install Security Manager Client. If Gen1 is not present, rename common instead. |
| <p>Error - Cannot Connect to Server</p> <p>The client cannot connect to the server. This can be caused by one of the following reasons: The server name is incorrect The protocol (http, https) is incorrect The server is not running Network access issues Please confirm the server name and protocol are correct the server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser.</p> | Most likely, the server is misconfigured for HTTPS traffic. | <ol style="list-style-type: none"> 1. From a browser, log in to the Cisco Security Management Suite desktop at https://<server>/CSCONm/servlet/login/login.jsp. 2. Click Server Administration. 3. In the Admin window, select Server > Security. 4. From the TOC, select Single Server Management > Browser-Server Security Mode Setup, then confirm that the Enable radio button is selected. If the radio button is not selected, select it now, then click Apply. 5. When prompted, restart the Cisco Security Manager Daemon Manager. 6. Wait 5 minutes, then try again to use Security Manager Client. If you still cannot connect, consider the other possible problems that the error message describes. |
| <p>Error - Cisco Security Agent Running</p> <p>Installation cannot proceed while the Cisco Security Agent is running</p> <p>Do you want to disable the Cisco Security Agent and continue with the installation?</p> | Cisco Security Agent needs to be stopped during the client installation. | <ul style="list-style-type: none"> • Click Yes to disable the Cisco Security Agent. • Click No to cancel the operation and stop the Cisco Security Agent manually. • Click Help to access online help for Security Manager client. |

Table A-3 **Installation Error Messages (Client) (continued)**

| Message | Reason for Message | User Action |
|---|---|--|
| <p>Error - Cisco Security Agent not Stopped</p> <p>The installation will be aborted because the Cisco Security Agent could not be stopped.</p> <p>Please attempt to disable Cisco Security Agent before repeating the installation process.</p> | <p>Security Manager client was unable to stop the Cisco Security Agent.</p> | <p>Click OK to close this error message and abort the installation. Manually disable the Cisco Security Agent before retrying the installation.</p> |
| <p>Error occurred during the installation: null.</p> | <p>Previous software installations and uninstalls caused InstallShield to run incorrectly.</p> | <ol style="list-style-type: none"> 1. Navigate to: C:\Program Files\Common Files\InstallShield\Universal\common\Gen1. 2. Rename the Gen1 folder, then try again to install Security Manager Client. If Gen1 is not present, rename common instead. |
| <p>Errors occurred during the installation.</p> <ul style="list-style-type: none"> • null | <p>Only a Windows user whose login account has administrative privileges can install Security Manager Client.</p> | <p>Log in as a Windows administrator, then try again to install Security Manager Client.</p> |
| <p>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.</p> | <p>If the OS on your client system is Windows 2003, its Internet Explorer Enhanced Security default settings might stop you from downloading the client software installation utility from your server.</p> | <ol style="list-style-type: none"> 1. Select Start > Control Panel > Add or Remove Programs. 2. Click Add/Remove Windows Components. 3. When the Windows Component Wizard window opens, deselect the Internet Explorer Enhanced Security Configuration check box, click Next, then click Finish. |
| <p>Please read the information below.</p> <p>The following errors were generated:</p> <ul style="list-style-type: none"> • WARNING: The <drive> partition has insufficient space to install the items selected. | <p>You tried to install Security Manager Client on a drive or partition that does not have enough free space.</p> | <p>Click Back, then select a different location in which to install Security Manager Client.</p> <p>Alternatively, see Changing the Default Location for Temporary Files, page C-3.</p> |
| <p>Unable to Get Data</p> <p>A database failure prevented successful completion of this operation.</p> | <p>You tried to use the client to connect to the server before the server database was completely up and running.</p> | <p>Wait a few minutes, then try again to log in. If the problem persists, verify that all required services are running.</p> |

- Q.** What should I do if the client installer suspends operation (hangs)?
- A.** Try the following. Any one of them might solve the problem:
 - If antivirus software is installed on your client system, disable it, then try again to run the installer.
 - Reboot the client system, then try again to run the installer.
 - Use a browser on the client system to log in to the Security Manager server at: **http://<server_name>:1741**. If you see an error message that says “Forbidden” or “Internal Server Error,” the required Tomcat service is not running. Unless you rebooted your server recently and Tomcat has not had enough time yet to start running, you might have to review server logs or take other steps to investigate why Tomcat is not running.

Problems After Installation

- Q.** Why is Security Manager Client missing from the Start menu in my Japanese version of Windows?
- A.** You might have configured the regional and language option settings to use English on the client system. We do not support English as the language in any Japanese version of Windows. Use the Control Panel to reset the language to Japanese.
- Q.** What can I do if my connections from a client system to the server seem unusually slow, or if I see DNS errors when I try to log in?
- A.** 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.)
- Q.** What is wrong with my authentication setup if my login credentials are accepted without any error message when I try to log in with Security Manager Client, but the Security Manager desktop is blank and unusable? (Furthermore, does the same problem explain why, in my web browser, Common Services on my Security Manager server accepts my login credentials but then fails to load the Cisco Security Management Suite desktop?)
- A.** You did not finish all of the required steps for Cisco Secure ACS to provide login authentication services for Security Manager and Common Services. Although you entered login credentials in ACS, you did not define the Security Manager server as a AAA client. You must do so, or you cannot log in. See the ACS documentation for detailed instructions.
- Q.** What should I do if I cannot use Security Manager Client to log in to the server and a message says...?

| | |
|--|---|
| <p>... repeatedly that the server is checking its license.</p> | <p>Verify that your server meets the minimum hardware and software requirements. See Server Requirements, page 2-4.</p> |
|--|---|

| | |
|--|--|
| <p>Synchronizing with DCR.</p> | <p>There are two possible explanations:</p> <ul style="list-style-type: none"> • You started Security Manager Client shortly after your server restarted. If so, allow a few more minutes for the server to become fully available, then try again to use Security Manager Client. • Your CiscoWorks administrative password contains special characters, such as ampersands (&). As a result, the Security Manager installation failed to create a comUser.dat file in the <i>NMSROOT</i>\lib\classpath subdirectory on your server, where <i>NMSROOT</i> is the directory in which you installed Common Services (the default is C:\Program Files\CSCOpX): <ol style="list-style-type: none"> a. Either contact Cisco TAC for assistance in replacing comUser.dat or reinstall Security Manager. b. Create a new Common Services password that does not use special characters. |
| <p>Error - Unable to Check License on Server.</p> <p>An attempt to check the license file on the Security Manager server has failed.</p> <p>Please confirm that the server is running. If the server is running, please contact the Cisco Technical Assistance Center.</p> | <p>At least one of the following services did not start correctly. On the server, select Start > Programs > Administrative Tools > Services, right-click each service named below, then select Restart from the shortcut menu:</p> <ul style="list-style-type: none"> • Cisco Security Manager Daemon Manager. • Cisco Security Manager database engine. • Cisco Security Manager Tomcat Servlet Engine. • Cisco Security Manager VisiBroker Smart Agent. • Cisco Security Manager Web Engine. <p>Wait 5 minutes, then try again to start Security Manager Client.</p> |

- Q.** Why is the Activity Report not displayed when I use Internet Explorer as my default browser?
- A.** This problem occurs because of invalid registry key values or inaccuracies with the location of some of the dll files 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>.

Other Problems

- Q.** I cannot install or uninstall any software on a client system. Why?
- A.** 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](#).

Troubleshooting the Standalone Security Agent

This section answers questions that you might ask about troubleshooting the standalone version of Cisco Security Agent that is installed in most cases when you install Security Manager server software.

- Q.** Under what circumstances might the standalone agent block network access to and from my server?
- A.** In broad terms, there are only two possibilities: Either malicious software is running on your server and the agent blocked it, or legitimate software on the server tried to do something that the agent misinterpreted as malicious. Both these problems can occur *only* if you previously set the agent security level to *high* and, in so doing, enabled an agent policy that is intended to detect and block the actions of untrusted rootkits. (The default setting is *medium*.)

We recommend that you investigate both possibilities to determine which of them is true in your case. Reading this log file should help you to identify the application whose actions the agent deemed suspicious: **C:\Program Files\Cisco Systems\CSAgent\log\csalog.txt**.

If your investigation shows that malicious software is running on the server, we recommend that you identify and eliminate whatever exploited vulnerabilities allowed the dangerous installation to occur. We further recommend that you wipe the server hard drive, then use the checklists and procedures in this guide to reinstall everything.

If you discover that benign (harmless) software—such as a trustworthy antivirus tool or a known device driver that loads dynamically after a system restart—triggered the agent, you can do any of the following:

- Reset the agent security level to *medium*, then restart the server.



Note If you later set the agent security level again to *high*, the agent again considers the trusted and reinstalled software to be untrustworthy and again blocks all network traffic.

- Uninstall the trusted software.
- Uninstall the agent. We recommend that you do never do this. See [Uninstalling the Standalone Agent, page B-3](#).
- Ask Cisco TAC to give you a revised agent. See [Obtaining Documentation and Submitting a Service Request, page xiv](#).

Another explanation is possible if the standalone agent blocks network access from your server. The Cisco Security Agent baseline policy for Windows users will not allow you to use Windows File Explorer to access any web page through HTTP.

- Q.** Why is Cisco Security Agent missing from the Start menu in my Japanese version of Windows?
- A.** You might have configured the regional and language option settings on the server to use English. We do not support English as the language in any Japanese version of Windows (see [Server Requirements, page 2-4](#)). Use the Control Panel to reset the language to Japanese.
- Q.** How can I verify that any Windows services that my standalone Cisco Security Agent might require are actually running on my server?
- A.** The standalone agent requires only one Windows service. Select **Start > Settings > Control Panel > Administrative Tools > Services**. You should see a running service called “Cisco Security Agent.”

- Q.** The red flag icon for Cisco Security Agent changed in my Windows system tray. The icon now has a red circle partially superimposed over it. What does it mean?
- A.** Something has disabled the agent (for example, you turned it off) or it is broken. Restarting your server might cause the standalone agent to reset itself, or you can check whether a message in the log tells you exactly what happened. See **C:\Program Files\CiscoSystems\CSAgent\log\csalog.txt**.
- Q.** The agent has blocked a valid operation. What can I do?
- A.** You can choose any of these possible workarounds:
- Right-click the agent icon in the Windows system tray, then select the *off* option to disable the agent temporarily. When you complete the task, reenabling the agent.
 - Uninstall the agent, even though we recommend that you do not uninstall it. See [Uninstalling the Standalone Agent, page B-3](#).
 - Select **Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent Diagnostics** to run the diagnostic utility.
- If none of the workarounds is sufficient, you can open a case with Cisco TAC (see [Obtaining Documentation and Submitting a Service Request, page xiv](#)).
- Q.** After I disable CSA so I can upgrade to a newer version of Security Manager, CSA is reenabled, causing the upgrade to fail. What must I do?
- A.** The CSA is “unclean.” You need to remove all registry entries for the strings "CSAgent" and "Cisco Security Agent," and remove all related program references and folders. See [Cleaning Up an Unclean Agent, page B-3](#).

Running a Server Self-Test

To run a self-test that confirms whether your Security Manager server is operating correctly:

Step 1 From a system on which Security Manager Client is connected to your Security Manager server, select **Tools > Security Manager Administration**.

Step 2 In the Administration window, click **Server Security**, then click any button. A new browser opens, displaying one of the security settings pages in the Common Services GUI, corresponding to the button you clicked.



Note If an error message is displayed when a new browser window opens, see [Configuring Required Client Settings To Open Browser Windows, page 6-2](#) for information on settings that can affect popup windows on systems where you use Security Manager Client.

Step 3 From the Common Services page, select **Admin** under the Server tab.

Step 4 In the Admin page TOC, click **Selftest**.

Step 5 Click **Create**.

Step 6 Click the **SelfTest Information at <MM-DD-YYYY HH:MM:SS>** link, where:

- *MM-DD-YYYY* is the current month, day, and year.
- *HH:MM:SS* is a timestamp that specifies the hour, minute, and second when you clicked Selftest.

- Step 7** Read the entries in the Server Info page.

Collecting Server Troubleshooting Information

The Security Manager Diagnostics utility collects server diagnostic information in a ZIP file, CSMDiagnostics.zip. You overwrite the file with new information each time you run Security Manager Diagnostics, unless you rename the file. The information in your CSMDiagnostics.zip file can help a Cisco technical support engineer to troubleshoot any problems that you might have with Security Manager or its related applications on your server.

You can run Security Manager Diagnostics in either of two ways.



Note

There is no requirement to submit a CSMDiagnostics.zip file when you first submit a problem report. In a case where we require the file, your Cisco technical support engineer tells you how to submit it.

| From a Security Manager client system: | From a Security Manager server: |
|--|--|
| <ol style="list-style-type: none"> After you establish a Security Manager Client session to your server, click Tools > Security Manager Diagnostics, then click OK. The CSMDiagnostics.zip file is saved on your server in the <i>NMSROOT\MDC\etc\</i> directory, where <i>NMSROOT</i> is the directory in which you installed Common Services (C:\Program Files\CSCOpX, for example). If you rename the file, you will not overwrite it accidentally. Click Close. | <ol style="list-style-type: none"> Select Start > Run, then enter command. Alternatively, if your server keyboard includes a Windows key, press Windows-R, then enter command. Enter C:\Program Files\CSCOpX\MDC\bin\CSMDiagnostics. Alternatively, to save the ZIP file in a different location than <i>NMSROOT\MDC\etc\</i>, enter CSMDiagnostics drive:\path. For example, CSMDiagnostics D:\temp. |

Viewing and Changing Server Process Status

To verify that the server processes for Security Manager are running correctly:

- Step 1** From the CiscoWorks home page, select **Common Services > Server > Admin**.
- Step 2** In the Admin page TOC, click **Processes**.

The Process Management table lists all server processes. Entries in the ProcessState column indicate whether a process is running normally.
- Step 3** If a required process is not running, restart it. See [Restarting All Processes on Your Server, page A-15](#).



Note

Only users with local administrator privileges can start and stop the server processes.

Restarting All Processes on Your Server

**Note**

You must stop all processes, then restart them all, or this method does not work.

Step 1

At the command prompt, enter **net stop crmdmgtd** to stop all processes.

Step 2

Enter **net start crmdmgtd** to restart all processes.

**Tip**

Alternatively, you can select **Start > Settings > Control Panel > Administrative Tools > Services**, then restart Cisco Security Manager Daemon Manager.

Reviewing the Server Installation Log File

If responses from the server differ from the responses that you expect, you can review error and warning messages in the server installation log file.

Use a text editor to open **C:\Ciscoverks_install_NNN.log**, where *NNN* is a timestamp in the format **YYYYMMDD_HHMMSS**.

In most cases, the log file to review is the one that has either the highest number appended to its filename or has the most recent creation date.

For example, you might see log file error and warning entries that say:

```
ERROR: Cannot Open C:\PROGRA~1\CSCOpX\lib\classpath\ssl.properties at
C:\PROGRA~1\CSCOpX\MDC\Apache\ConfigSSL.pl line 259.
INFO: Enabling SSL....
WARNING: Unable to enable SSL. Please try later....
```

**Note**

In the event of a severe problem, you can send the log file to Cisco TAC. See [Obtaining Documentation and Submitting a Service Request](#), page xiv.

