



## Troubleshooting

---



### Note

CiscoWorks Common Services 3.0.3 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 the Installation” in the Common Services online help or read it on Cisco.com: [http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_common\\_services\\_software/3.0.3/installation/windows/guide/appenda.html](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_common_services_software/3.0.3/installation/windows/guide/appenda.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-2](#)
- [Troubleshooting the Standalone Security Agent, page A-11](#)
- [Running a Server Self-Test, page A-13](#)
- [Collecting Server Troubleshooting Information, page A-13](#)
- [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 successfully:

- [Server Q&A, page A-2](#)
- [Client Q&A, page A-7](#)

## Server Q&A

- 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](#), 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"> <li>1. Shut down the server, then restart it.</li> <li>2. Use a Registry editor to delete this entry: \$HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager\CurrentVersion.</li> <li>3. In the directory where you installed Security Manager, create a subdirectory named <i>setup</i>.</li> <li>4. If it exists, delete the CMFLOCK.TXT file.</li> <li>5. Reinstall Security Manager.</li> </ol>

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

Message	Reason for Message	User Action
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.
Severe  Failed on call to FileInsertLine.	Your server does not meet the requirement for hard drive space.	See <a href="#">Server Requirements, page 1-4</a> .
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 <a href="#">Readiness Checklist for Installation, page 1-5</a> .	<ol style="list-style-type: none"> <li>1. Disable Terminal Services. To learn how to do this, see the “<a href="#">Terminal Server Support for Windows 2000 and Windows 2003 Server</a>” topic in <i>Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView) on Windows</i>.</li> <li>2. Try again to install Security Manager.</li> </ol>

**Note** For additional information about installation error messages, see the Common Services 3.0.3 documentation on Cisco.com.

- Q.** What should I do if the server installer suspends operation (hangs)?
- A.** Reboot and try again.

- Q.** Can Security Manager 3.0.1 coexist on a server with any older version of Common Services than 3.0.4?
- A.** No. As of June 2006, we do not support coexistence on the same server with any Common Services version older than 3.0.4. However, we might support newer Common Services versions later.

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

- 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 1-9](#).
  - Your server uses the wrong Windows language. Only English and Japanese are supported. (See [Server Requirements, page 1-4](#).) 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 either US-English or Japanese, then uninstall and reinstall Security Manager. See [Uninstalling and Reinstalling Server Applications, page 1-11](#).
  - 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-11](#).

- You ran the Security Manager installation utility over a network connection, but we do not support this use case (see [Installing or Upgrading Server Applications, page 1-3](#)). You must uninstall and reinstall the server software. See:
    - a. [Uninstalling Server Applications, page 1-12](#).
    - b. [Reinstalling Server Applications, page 1-13](#).
  - Your client system does not meet the minimum requirements. See [Client Requirements, page 1-7](#).
  - 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 1-7](#).
- 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.** 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 1-5](#). To work around this problem, reset the server date/time settings.

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

**Table A-2 Uninstallation Error Messages**

Message	Reason for Message	User Action
D:\temp\ <i>&lt;subdirectory&gt;</i> \ setup.exe - Access is denied.  The process cannot access the file because it is being used by another process.  0 file(s) copied. 1 file(s) copied.	Uninstallation failed.	Reboot the server, then complete the procedure described in <a href="#">Uninstalling Server Applications</a> , page 1-12.

**Note** For additional information about uninstallation error messages, see the Common Services 3.0.3 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*d service is not responding and asks “Do you want to keep waiting?”
- A.** The uninstallation script includes an instruction to stop the *crmdmgt*d service, which did not respond to that instruction before the script timed out. Click **Yes**. In most cases, the *crmdmgt*d service then stops as expected.

## Client Q&A

- 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"> <li>1. Navigate to: <b>C:\Program Files\ Common Files\ InstallShield\Universal\ common\Gen1.</b></li> <li>2. Rename the Gen1 folder, then try again to install Security Manager Client.  If Gen1 is not present, rename <b>common</b> instead.</li> </ol>
Error occurred during the installation: null.	Previous software installations and uninstallations caused InstallShield to run incorrectly.	<ol style="list-style-type: none"> <li>1. Navigate to: <b>C:\Program Files\ Common Files\ InstallShield\Universal\ common\Gen1.</b></li> <li>2. Rename the Gen1 folder, then try again to install Security Manager Client.  If Gen1 is not present, rename <b>common</b> instead.</li> </ol>
Errors occurred during the installation. <ul style="list-style-type: none"> <li>• null</li> </ul>	Only a Windows user whose login account has administrative privileges can install Security Manager Client.	Log in as a Windows administrator, then try again to install Security Manager Client.

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

Message	Reason for Message	User Action
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.	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.	<ol style="list-style-type: none"> <li>1. Select <b>Start &gt; Control Panel &gt; Add or Remove Programs</b>.</li> <li>2. Click <b>Add/Remove Windows Components</b>.</li> <li>3. When the Windows Component Wizard window opens, deselect the <b>Internet Explorer Enhanced Security Configuration</b> check box, click <b>Next</b>, then click <b>Finish</b>.</li> </ol>
<p>Please read the information below.</p> <p>The following errors were generated:</p> <ul style="list-style-type: none"> <li>• WARNING: The &lt;drive&gt; partition has insufficient space to install the items selected.</li> </ul>	You tried to install Security Manager Client on a drive or partition that does not have enough free space.	<p>Click <b>Back</b>, then select a different location in which to install Security Manager Client.</p> <p>Alternatively, see <a href="#">Changing the Default Location for Temporary Files, page 1-2</a>.</p>
<p>Unable to Get Data</p> <p>A database failure prevented successful completion of this operation.</p>	You tried to use the client to connect to the server before the server database was completely up and running.	Wait a few minutes, then try again to log in. If the problem persists, verify that all required services are running.

**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 Norton Internet Security 2005 is installed, 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.
- Q.** What should I do if I cannot use Security Manager Client to log in to the server, and a repeating message tells me the server is checking its license?
- A.** Verify that your server meets the minimum hardware and software requirements. See [Server Requirements, page 1-4](#).
- Q.** My client system uses Windows 2000 as its operating system and its copy of Internet Explorer shows page display errors when I try to establish connections to a Security Manager server. What is the problem?
- A.** Security Manager uses and requires a cipher strength of 128 bits for SSL communication. Internet Explorer cannot use 128-bit encryption on systems that run Windows 2000 without Service Pack 4. If your client system uses Windows 2000 without Service Pack 4, its copy of Internet Explorer uses 56-bit encryption for SSL connections, and therefore cannot communicate with any Security Manager server. For a complete description of the system requirements to use Security Manager Client, see [Client Requirements, page 1-7](#).

**Tip**

---

To learn what cipher strength your client system uses in its copy of Internet Explorer, select **Help > About Internet Explorer**.

---

- Q.** I am unable to 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](#).

- Q.** When I uninstall the client software, what does this uninstallation error message mean?
- A.** Client software uninstallation error messages and explanations appear in [Table A-4](#), where they are sorted alphabetically by their first word.

**Table A-4**      **Uninstallation Error Messages (Client)**

Message	Reason for Message	User Action
Welcome to the InstallShield Wizard for ERROR: cannot load product /product.xml	The uninstall.dat file is not in its expected location, or was deleted.	<ul style="list-style-type: none"> <li>• If you moved the uninstall.dat file, return it to the specified folder, then try again to use the uninstallation utility.</li> <li>• If you deleted uninstall.dat, but you know that another client system is using the identical version of Security Manager Client<sup>1</sup>, copy the required file from that other system to the specified folder where the file is missing, then try again to use the uninstallation utility.</li> <li>• If you deleted uninstall.dat and have no other copy of it, do the following:               <ol style="list-style-type: none"> <li>1. Delete the directory in which you installed Security Manager Client.</li> <li>2. Rename the C:\Program Files\Common Files\InstallShield\Universal\Gen1 subdirectory.</li> <li>3. Install a new copy of Security Manager Client.</li> </ol> </li> </ul>

**Note** For additional information about uninstallation error messages, see the Common Services 3.0.3 documentation on Cisco.com.

1. You can assume that the uninstall.dat files for Security Manager Client are identical on two client systems when you see identical values in the client.info files on those same two systems. To check whether the values are identical, use any text editor to read the **client.info** file, which is located by default in the directory where you installed Security Manager Client. The relevant values in the file use these labels: PRODVERS, VERSION, PATCHVER, and BUILD\_NUM.

# 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 will again consider the trusted and reinstalled software to be untrustworthy and will again block all network traffic.

---

- Uninstall the trusted software.
- Uninstall the agent. We recommend that you do never do this. See [Uninstalling the Standalone Agent, page A-4](#).
- Ask Cisco TAC to give you a revised agent.

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.** 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. A message in the log might tell you exactly what happened. See **C:\Program Files\Cisco Systems\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, reenable the agent.
  - Uninstall the agent, even though we recommend that you do not uninstall it. See [Uninstalling the Standalone Agent, page A-4](#).
  - 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.
- Q.** If I upgrade Security Manager from 3.0 to 3.0.1, what happens to my Security Agent log files from Security Manager 3.0?
- A.** The log files are retained in C:\Program Files\Cisco Systems\CSAgent\log\.

# 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.
  - Step 3** When a new browser opens, click the **CiscoWorks** link.
  - Step 4** From the Common Services area on the CiscoWorks home page, select **Server > Admin**.
  - Step 5** In the Admin page TOC, click **Selftest**.
  - Step 6** Click **Create**.
  - Step 7** 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 8** 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 Cisco requires the file, your 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"> <li>After you establish a Security Manager Client session to your server, click <b>Tools &gt; Security Manager Diagnostics</b>, then click <b>OK</b>.  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.</li> <li>Click <b>Close</b>.</li> </ol>	<ol style="list-style-type: none"> <li>Select <b>Start &gt; Run</b>, then enter <b>command</b>. Alternatively, if your server keyboard includes a Windows key, press <b>Windows-R</b>, then enter <b>command</b>.</li> <li>Enter <b>C:\Program Files\CSCOPx\MDC\bin\CSMDiagnostics</b>. Alternatively, to save the ZIP file in a different location than <i>NMSROOT\MDC\etc\</i>, enter <b>CSMDiagnostics drive:\path</b>. For example, CSMDiagnostics D:\temp.</li> </ol>

## 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\_setupNNN.log**, where *NNN* is a three-digit number that counts the number of Security Manager (or CiscoWorks-related) installations over time. A log file for which the filename ends in *018* therefore describes a more recent installation than is described in a log file for which the filename ends in *017*.

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.

---

