



CHAPTER 1

Security Manager Server

This chapter contains the following topics:

- [Collecting Server Troubleshooting Information, page 1-1](#)
- [Security Manager Database, page 1-2](#)
- [Restoring the Database Using Backed-Up Files](#)
- [Unable to Launch the Security Manager Server, page 1-3](#)
- [Restricting Access to the Security Manager Server, page 1-4](#)
- [Installation, Uninstallation, or Reinstallation, page 1-4](#)



Note

For detailed information on installing and uninstalling the Security Manager Server, see the [installation guide for Cisco Security Manager](#) for your release.

Collecting Server Troubleshooting Information

If you are experiencing problems with Security Manager, and you cannot resolve the problem after trying all the recommendations listed in the error message and reviewing this guide for a possible solution, use the Security Manager Diagnostics utility to collect server information.

The Security Manager Diagnostics utility collects server diagnostic information in a ZIP file (CSMDiagnostics.zip) that you overwrite with new information each time you run Security Manager Diagnostics. 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.



Tip

Security Manager also includes an advanced debugging option that collects information about the configuration changes that have been made with the application. To activate this option, select **Tools > Security Manager Administration > Deployment**, then select the **Enabled Advanced Debugging** check box. Bear in mind that although the additional information saved to the diagnostics file may aid the troubleshooting effort, the file may contain sensitive information, such as passwords.



Note

There is no requirement to submit a CSMDiagnostics.zip file when you first submit a problem report. Your support engineer provides you with a method to submit the file if it is required.

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

From a Security Manager client system:	From a Security Manager server:
<ol style="list-style-type: none"> 1. On a client system from which you have established a Security Manager Client session to your server, click Tools > Security Manager Diagnostics. 2. Click OK to generate the diagnostics file. The resulting ZIP file (CSMDiagnostics.zip) is saved on your server in the <i>NMSROOT\MDC\etc\</i> directory, where <i>NMSROOT</i> is the directory where you installed Common Services (C:\Program Files\CSCOpX, for example). 3. Click Close to close the Security Manager Diagnostics dialog box. <p>Note We recommend that you rename this file so it does not get overwritten each time you run this utility.</p>	<ol style="list-style-type: none"> 1. Select Start > Run, then enter command. Alternatively, if your server keyboard includes a Windows key, press Windows-R, then enter command. 2. 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.

Security Manager Database

This procedure describes the steps to take if you are having problems with the Security Manager database or if the database is corrupted.

Procedure

-
- Step 1** Back up the database:
- a. Select **Tools > Backup**. The Backup Job page of CiscoWorks Common Services is displayed in a browser window.
 - b. Select a backup directory and schedule the operation.
 - c. Click **Apply**.



Note Security Manager is shut down during the backup process. This is to prevent any inconsistency between different databases and data files. For complete details, click **Help** in the Common Services window to view the online help topic for “Scheduling a Backup”.

- Step 2** Send the database to TAC for troubleshooting.
- Step 3** After TAC corrects the problem and sends the database back to you, restore it in your system. For details, see “Backing up and Restoring the Security Manager Database” in the *Managing the Security Manager Server* chapter of the User Guide for your release:
- http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
- Step 4** Change the database password.

For the procedure, see “Changing the Database Password” in the CiscoWorks Common Services online help. For quick results, access the online help and use the search function to find this topic.

Restoring the Database Using Backed-Up Files

Problem You want to restore a backup from a set of files that were not created using the backup mechanism in CiscoWorks Common Services.

Solution Restoring the Security Manager database directly from backed up files introduces a variety of potential problems, including hostname issues, file permission issues, database password issues, and file consistency issues. Therefore, we strongly recommend using the backup and restore mechanism in CiscoWorks Common Services to restore the Security Manager database.

Restoring the Database from a Previous Version of Security Manager

Problem You want to restore a database that was backed up prior to installing service packs.

Solution If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.

Unable to Launch the Security Manager Server

Problem When you try to launch Security Manager, you receive a message that indicates you do not have permission to access /cwhp/LiaisonServlet on the Security Manager server.

Solution [Table 1-1](#) describes common causes and suggested workarounds for this problem.

Table 1-1 Causes and Workarounds for LiaisonServlet Error

Cause	Workaround
Anti-virus application installed on server	Uninstall the anti-virus application.
IIS installed on server	As stated in the <i>Installation Guide for Cisco Security Manager</i> , IIS is not compatible with Security Manager and must be uninstalled.
Services required by Security Manager do not start in proper order	The only service that should be set to Automatic is the Cisco Security Manager Daemon Manager. All other CiscoWorks services should be set to Manual. Please note that it may take the Daemon Manager a few minutes to start up the other CiscoWorks services. These services must start up in the proper order; manually starting up the services can cause errors.
casuser password	The casuser login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. Reset the casuser password as follows: <ol style="list-style-type: none"> 1. Open a command line. 2. Type <code>C:\Program Files\CSCOpX\setup\support\resetCasuser.exe</code>, then press Enter. 3. Choose option 1 (Randomly generate casuser password).

Restricting Access to the Security Manager Server

Problem You want to restrict access to the Security Manager server to a defined number of hosts based on the client IP address.

Solution Assuming that Security Manager is configured as part of a NOC (network operations center), you can configure ACLs on the firewall or router that acts as the perimeter device between the NOC and the other hosts. The ACLs should permit access to the Security Manager server over ports 443 and 1741 to specific IP addresses only. If Security Manager is managing the perimeter device, you can define these ACLs in an Access Rules policy and deploy the policy to the device.

Installation, Uninstallation, or Reinstallation

See the “Troubleshooting” chapter in 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.