# Troubleshooting

CiscoWorks Common Services provides Security Manager with its framework for installation, uninstallation, and re-installation 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.

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




# Troubleshooting

CiscoWorks Common Services provides Security Manager with its framework for installation, uninstallation, and re-installation 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.

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

- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF
- XREF

# Startup Requirements for 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 ensures that all the related services are stopped and started in the correct order.

# Comprehensive List of Required TCP and UDP Ports

The Cisco Security Management Suite applications need to communicate with clients and other applications. Other server applications might be installed on separate computers. For successful communication, certain TCP and UDP ports need to be open and available for transmitting traffic. Normally, you need to open only those ports described in Required Services and Ports. However, if you find that the applications are not able to communicate, the following table describes additional ports that you might need to open. The list is in port number order.

*Table 1: Required Services and Ports*

| Service | Used For, or Used By | Port Number/Range of Ports | Protocol | Inbound | Outbound |
|---|---|---|---|---|---|
| FTP | Security Manager communication with TMS server | 21 | TCP | — | X |
| SSH | Common Services | 22 | TCP | — | X |
| | Security Manager | 22 | TCP | — | X |
| Telnet | Security Manager | 23 | TCP | — | X |
| SMTP | Common Services | 25 | TCP | — | X |
| TACACS+ (for ACS) | Common Services | 49 | TCP | — | X |
| TFTP | Common Services | 69 | UDP | X | X |
| HTTP | Common Services | 80 | TCP | — | X |
| | Security Manager | | TCP | — | X |
| SNMP (polling) | Common Services | 161 | UDP | — | X |
| | Performance Monitor | 161 | UDP | — | X |
| SNMP (traps) | Common Services | 162 | UDP | — | X |
| | Performance Monitor | 162 | UDP | X | — |
| HTTPS (SSL) | Common Services | 443[1] | TCP | X | — |
| | Security Manager | | TCP | X | X |
| | Performance Monitor | | TCP | X | — |
| | Syslog[2] | | Security Manager | 514 | UDP | X | — |
| Common Services (without Security Manager installed) | | 514 or 49514 (see footnote for this row) | UDP | X | — |
| Performance Monitor (without Security Manager installed) | | 514 | UDP | X | — |
| Remote Copy Protocol | Common Services | 514 | TCP | X | X |

| Service | Used For, or Used By | Port Number/Range of Ports | Protocol | Inbound | Outbound |
|---|---|---|---|---|---|
| HTTP | Common Services | 1741 | TCP | X | — |
| | Security Manager | | TCP | X | — |
| | Performance Monitor | | TCP | X | — |
| | RADIUS<br>LDAP<br>Kerberos | | Security Manager (to external AAA server) | 1645, 1646, 1812(new), 389, 636 (SSL), 88 | TCP — X |
| Access Control Server HTTP/HTTPS | Security Manager | 2002 | TCP | — | X |
| HIPO port for CiscoWorks gatekeeper | Common Services | 8088 | TCP | X | X |
| Tomcat shutdown | Common Services | 9007 | TCP | X | — |
| Tomcat Ajp13 connector | Common Services | 9009 | TCP | X | — |
| Database | Security Manager | 10033 and 10034 | TCP | X | — |
| License Server | Common Services | 40401 | TCP | X | — |
| Daemon Manager | Common Services | 42340 | TCP | X | X |
| Osagent | Common Services | 42342 | UDP | X | X |
| Database | Common Services | 43441 | TCP | X | — |
| Performance Monitor | 43453 | TCP | X | X | |
| DCR and OGS | Common Services | 40050 – 40070 | TCP | X | — |
| Event Services | Software Service | 42350/44350 | UDP | X | X |
| | Software Listening | 42351/44351 | TCP | X | X |
| | Software HTTP | 42352/44352 | TCP | X | X |
| | Software Routing | 42353/44353 | TCP | X | X |
| Transport Mechanism (CSTM) | Common Services | 50000 – 50020 | TCP | X | — |

[1] To share and exchange information with a Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance, Security Manager uses HTTPS over port 443 by default. You can choose whether to use a different port for this purpose.

[2] During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514.

# CSM 4.26 Upgrade Troubleshooting

The following topics help you to troubleshoot problems that might occur when you upgrade your Security Manager.



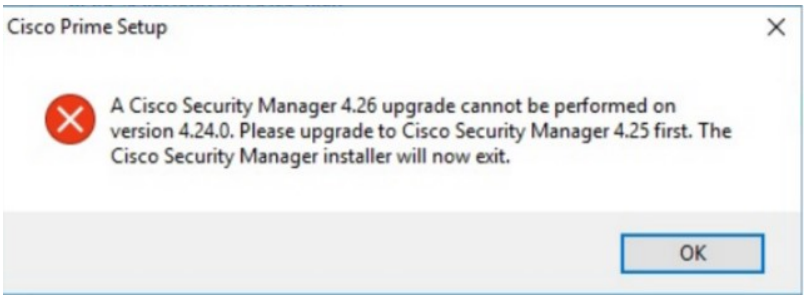
## Troubleshooting Logs

You can refer to the migration logs for troubleshooting migration issues that occur during CSM 4.26 installation.

- Refer to the migration logs export_tables_mariadb_migration.log and import_tables_mariadb_migration.log available in CSCOpx\log.
- You can use the data migration logs to troubleshoot the migration issues that occur while exporting the data from SQLAnywhere database to Maria database.
- Export migration logs: migration logs print **Import Process encounters Issue!!**(export_tables_sybasedb.pl - import_tables_mariadb_migration.log) in case there is an issue in the export migration.
- Import migration logs: migration logs print **Export Process encounters Issue!!**(import_tables_mariadb.pl - export_tables_mariadb_migration.log) in case there is an issue in the import migration.
- Installation and Uninstallation errors are in the following logs present under C:\ Drive
  - Cisco_Prime_install_<time stamp>.log [ CSM Install log ]
  - Cisco_Prime_uninstall_<time stamp>.log [ CSM Uninstall log ]

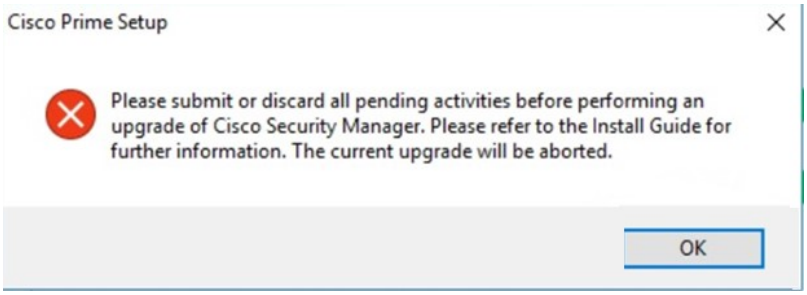
## Version Upgrade Validation

You can upgrade your CSM to 4.26 version only from 4.25. You will encounter an error if you try to upgrade your Security Manager directly from a version below 4.25. In addition, only inline upgrade is supported from 4.25 to 4.26.




# Data Validation Check

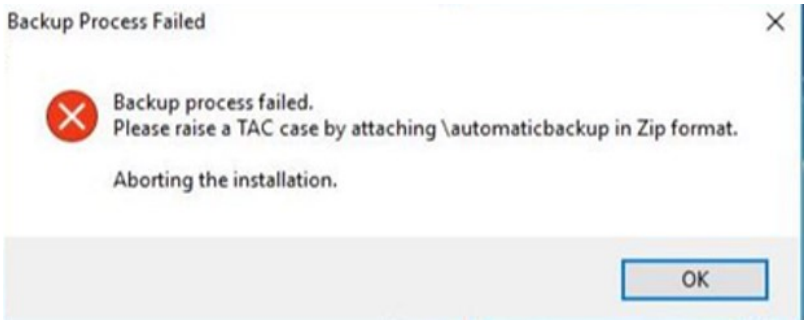
During inline upgrade from 4.25 to 4.26, Security Manager checks for the pending activity after the WMI check warning you to commit or discard the pending activities to proceed further with the upgrade.




# Backup Process Validation

If the backup fails during the backup process, CSM 4.26 installation checks the log and throws the following validation error popup and then aborts the installation.

```
Backup process failed. Please raise a TAC case by attaching
C:\Progra~2\425_backup\automaticbackup in Zip format. Aborting the installation.
```

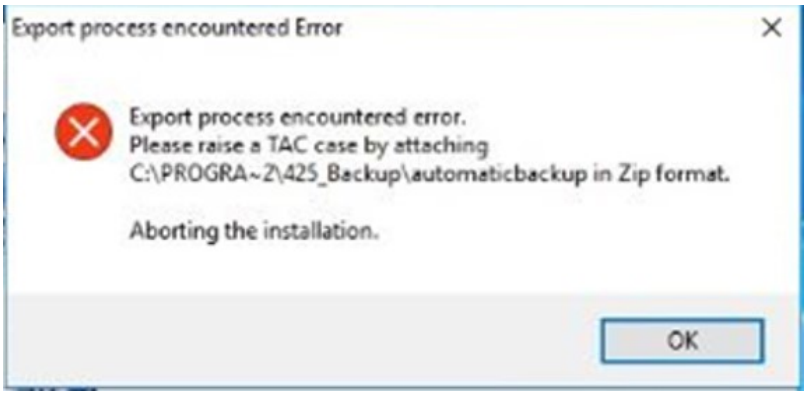



**Note** You can continue using CSM 4.25 until you get a reply from the Technical team.

# Export Process Validation

If the export DB encounters an error in the process during the database export, the installation will display the following error message and then aborts the Installation.

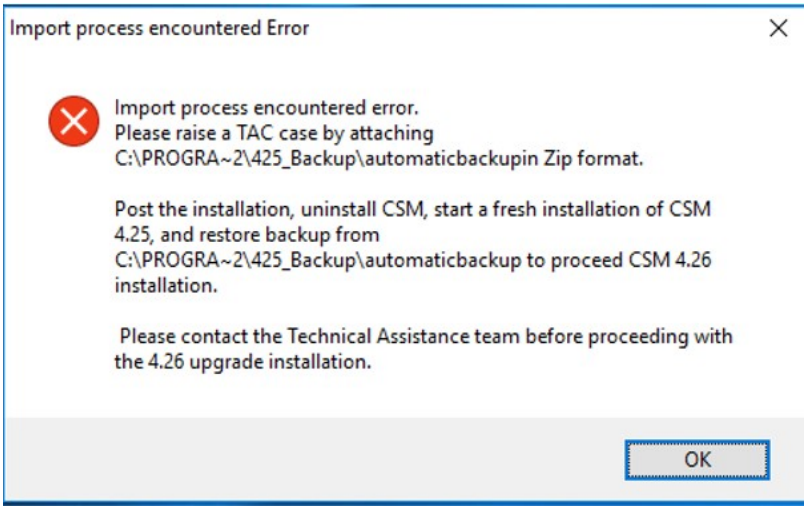
```
Export process encountered error. Please raise a TAC case by attaching
C:\Progra~2\425_Backup\automaticbackup in Zip format. Aborting the installation.
```




# Import Process Validation

If the import DB encounters an error in the process during the database import, the installation will display the following error message and then aborts the Installation.

```
Import process encountered error. Please raise a TAC case by attaching
C:\Progra~2\425_Backup\automaticbackup in Zip format. Aborting the installation.
```




# Password Validation

When you face this issue you can click **OK** to proceed with the upgrade. Once the upgrade completes and the system restarts, you must execute the following steps before logging in. And, you must follow the following password requirements while setting password for the database.

If you are an existing user and do not meet the password limitation, then the Security Manager 4.26 throws a validation message during installation. Based on the error popup, you must manually reset the password using dbpasswd.pl commad. Error message displays the database (vms or rpt or cmf) that does not meet the limitation for which you must execute the command.

**NMSROOT\bin\perl NMSROOT\bin\dbpasswd.pl dsn=<DB name> npwd=<new_password>**

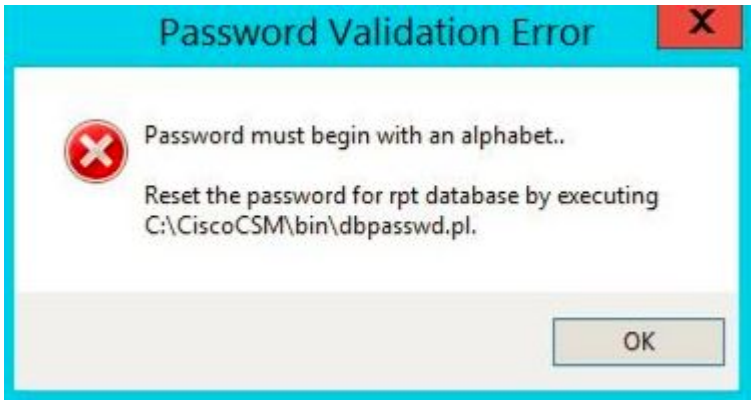
For example, **C:\PROGRA~2\CSCOpx\bin\perl C:\PROGRA~2\CSCOpx\bin\dbpasswd.pl dsn=vms npwd=cisco**

- Password must contain atleat 5 characters long


- Only characters A-Z, a-z, 0-9 are allowed


- Password should contain fewer than 30 characters

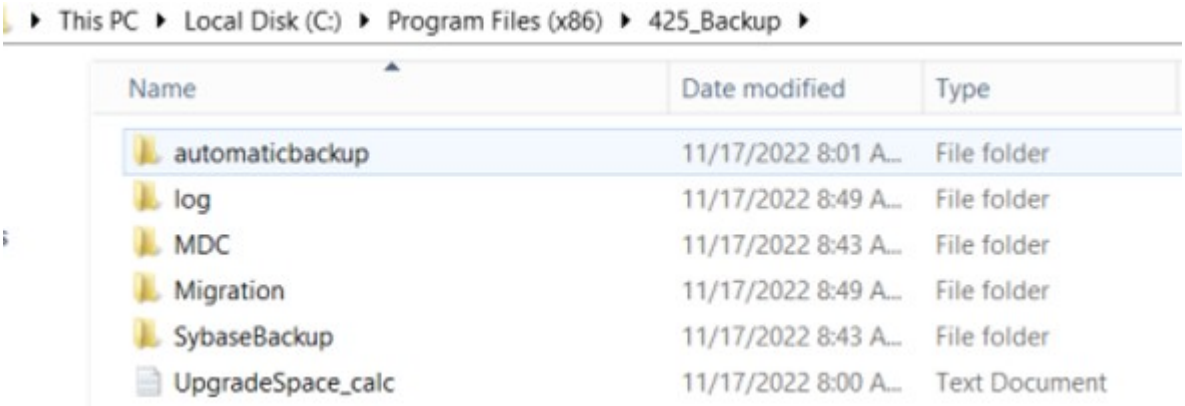

- Password must begin with an alphabet




# Troubleshooting Export Process

Follow the below steps to troubleshoot the inline upgrade failure that occurs during the backup process.

**Step 1** Contact the Technical team attaching the backup from the location **C:\Progra~2\425_backup\automaticbackup** in .zip format.



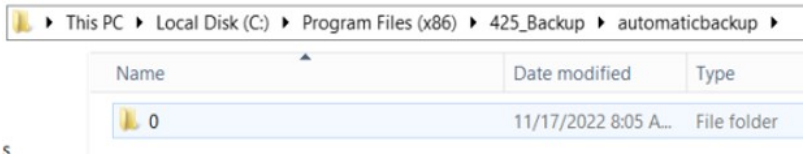
**Step 2** Start the Daemon Manger and proceed with CSM 4.25 until you get a reply from the CSM Technical team.

**Note** The CSM installed location has the backup folder (425_backup folder). If you install the CSM in a custom drive for example **C:\CSM\Cisco**, then the 425_backup folder appears in **C:\CSM\425_Backup**.

# Troubleshooting Import Process

Follow the below steps to troubleshoot the inline upgrade failure that occurs during the import process.

**Step 1** Contact the Technical team attaching the backup from the location **C:\Progra~2\425_backup\automaticbackup** in .zip format.




**Step 2** Uninstall the current CSM, re-install 4.25 and restore the backup from (**C:\Progra~2\425_backup\automaticbackup**) with the following restore command to bring up the CSM 4.25 Server.

```
<CSM installed directory>\bin\perl <CSM installed directory>\bin\restorebackup.pl -d <backup Dir>
```

**Example:**

C:\Progra~2\CSOCpx\bin\perl C:\Progra~2\CSOCpx\bin\restorebackup.pl –d C:\Progra~2\425_backup\automaticbackup

# Troubleshooting the Security Manager Server

This section answers questions that you might have about:


- Server Problems During Installation , on page 10
- Server Problems After Installation , on page 13
- Server Problems During Uninstallation , on page 16


## Server 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 2: Installation Error Messages (Server) , where they are sorted alphabetically by their first word.

*Table 2: 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. | 1. Shut down the server, then restart it.<br>2. Use a Registry editor to delete this entry: $HKEY_LOCAL_MACHINE\SOFTWARE\Wow643<br>3. In the directory where you installed Security Manager<br>4. Delete CMFLOCK.TXT if it exists.<br>5. Re-install 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. |
| `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 install |

| Message | Reason for Message | User Action |
|---|---|---|
| The Windows 2012 R2 server may not have the following Microsoft Windows patches:<br>a. KB2919442<br>b. Run clearcompressionflag.exe<br>c. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018<br>d. KB2999226<br>These patches are required to register critical Cisco Security Manager services in this server. Ensure that you install these patches in the aforesaid order.<br>We recommend you to install these patches before installing the Cisco Security Manager. Alternatively, you can also install these patches after installing the Cisco Security Manager, and then run the "<CSMInstalledDirectory>\CSCOpx\bin\RegisterApache.bat" CSM scripts to register the services.<br>For more information, refer the Installation Guide for Cisco Security Manager.<br>To continue with installation, click OK.<br>To abort the installation, click Cancel. | The recommended Windows Update patches may be missing in your Windows 2012 R2 server. | Ensure you have the required patches installed in your server,<br>You may proceed installing Cisco Security Manager, and ther to register Apache Services with the windows services.<br>For more information, refer Readiness Checklist for Installati |
| 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`<br>`Failed on call to FileInsertLine.` | Your server does not meet the requirement for hard drive space. | See Server Requirements and Recommendations. |
| `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 subdirectori all such subdirectories. |

| Message | Reason for Message | User Action |
|---|---|---|
| `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 XREF. | 1. Disable Terminal Services.<br>To learn how to do this, see the "Terminal Server Support *Installing and Getting Started With CiscoWorks LAN Man*<br>http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_<br>1. 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. | 1. Verify that you have appropriate permissions to write done by a member of local administrators group.<br>2. Click **OK** to close the error message, log out of Windo has local administrator privileges. |

**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.** Why does the Security Manager database backup fail?

**A.**If network management applications, such as Tivoli, were used to install Cygwin on the same system where a Security Manager server was installed, backup of the Security Manager database fails. Uninstall Cygwin.

# Server Problems After Installation

**Q.** I want to change the hostname of the Security Manager Server. How do I achieve this?

**A.**You can change the hostname of the Security Manager Server by performing the steps detailed in (Optional) Changing the Hostname of the Security Manager Server.

**Q.** The Security Manager interface does not appear, or is not displayed correctly, or certain interface 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 interface:

- 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.
- 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 and Recommendations.) 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 re-install Security Manager. See Uninstalling Server Applications.
- You ran the Security Manager installation utility over a network connection, but we do not support this use case (see Installing Security Manager Server and Common Services). You must uninstall and re-install the server software. See Uninstalling Server Applications.
- Your client system does not meet the minimum requirements. See Client Requirements.
- 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.

**Problem** When trying to open web interface to Security Manager using a web browser, a message indicates that I do not have permission to access /cwhp/LiaisonServlet on the Security Manager server. What does this mean?

**Solution** The following table describes common causes and suggested workarounds for this problem.

***Table 3: Causes and Workarounds for LiaisonServlet Error***

| Cause | Workaround |
|---|---|
| Anti-virus application installed on server | Uninstall the anti-virus application. |
| IIS installed on server | 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. |

| Cause | Workaround |
|---|---|
| casuser password | The following five permissions are assigned and set, automatically, at the time of Security Manager installation:<br>• Access this computer from network - casusers<br>• Deny access to this computer from network - casuser<br>• Deny logon locally - casuser<br>• Log on as batch job - casuser, casusers<br>• Log on as a service – casuser<br>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:<br>**1.** Open a command prompt on the server using the Run as administrator option.<br>**2.** Type NMSRoot\setup\support\resetCasuser.exe and then press **Enter**.<br>**Note** The location NMSROOT is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx**.<br>**3.** Of the two option displayed, choose option 2 - Enter casuser password. You will be prompted to enter a password for casuser and then to reenter the password for confirmation.<br>**4.** If local security policy is configured, add the casuser account to the 'Log on as a service' operation in the local security policy.<br>**5.** Run the following command to apply the casuser permission to *NMSROOT* : C:\Windows\System32\cacls.exe "NMSROOT" /E /T /G Administrators:F casusers:F<br>**6.** Run the following command to set the casuser to database services:NMSROOT\bin\perl NMSROOT\bin\ChangeService2Casuser.pl "casuser" "casuserpassword" |

**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. You must place any files you need to select in Security Manager on the server, such as license files.

**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 and Recommendations). 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. 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 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. The client must use whatever protocol the server is configured to use.

**Q.** I am using a VMware setup, and system performance is unacceptably slow, for example, system backup takes two hours.

**A.**Ensure that you allocate two or more CPUs to the VM running Security Manager. Systems allocating one CPU have been found to have unacceptable performance for some system activities.

**Q.** Validation and some other operations fail with SQL query for MariaDB exception in logs. What happened?

**A.**If the TMPDIR, TEMP, or TMP are not set, MySQL for Maria DB uses the Windows system default, which is usually **C:\windows\temp** . If the file system containing your temporary file directory is too small, you can use the mysqld--tmpdir option to specify a directory in a file system where you have enough space.

**Q.**I want to enable 2048 bit for Diffie-Hellman but I couldn't find a way to do it.

**A.**Apache supports 512 bit by default and does not support 2048 bit since this Dhparam needs parameter modification during compilation which is not possible in CSM. Hence, you cannot enable the 2048 bit for Diffie-Hellman in CSM 4.22.

# Server Problems During Uninstallation

**Q.** What does this uninstallation error message mean?

**A.**Uninstallation error messages and explanations appear in Table 4: Uninstallation Error Messages , where they are sorted alphabetically by their first word. For additional information about uninstallation error messages, see the Common Services documentation in your installation of Security Manager.

*Table 4: Uninstallation Error Messages*

| Message | Reason for Message | User Action |
|---|---|---|
| C:*NMSROOT*<br>\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:<br>- Simple file sharing is enabled in Windows.<br>- 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:<br>**Simple File Sharing**<br>1. Select **Start > Settings > Control Panel > Folder Options**.<br>2. Click the **View** tab.<br>3. Scroll to the bottom of the Advanced Settings pane.<br>4. Uncheck the **Use simple file sharing (Recommended)** check box, then click **OK**.<br>**Offline File Synchronization**<br>1. Select **Start > Settings > Control Panel > Folder Options**.<br>2. Click the **Offline Files** tab.<br>3. Uncheck the **Enable Offline Files** check box, then click **OK**. |
| C:\temp\<*subdirectory*<br>>\setup.exe - Access is denied.<br>The process cannot access the file because it is being used by another process.<br>0 file(s) copied.1 file(s) copied. | Uninstallation failed. | Reboot the server, then complete the procedure described in Uninstalling Server Applications. |
| Windows Management Instrumentation (WMI) is running.<br>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.<br>Do you want to proceed?<br>Click Yes to proceed with this uninstallation. Click No to exit uninstallation. | Either your organization uses WMI or someone enabled the WMI service accidentally on your server. | Click **Yes**. |

**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 *crmdmgtd* service is not responding and asks "Do you want to keep waiting?"

**A.**The uninstallation script includes an instruction to stop the crmdmgtd service, which did not respond to that instruction before the script timed out. Click **Yes**. In most cases, the crmdmgtd service then stops as expected.

# Troubleshooting the Security Manager Client

This section answers questions that you might have about:


- Client Problems During Installation , on page 18
- Client Problems After Installation , on page 21


## Client 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 5: Installation Error Messages (Client) , where they are sorted alphabetically by their first word.

***Table 5: 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. | 1. Navigate to: **C:\Program Files (x86)\Common Files\InstallShield\Universal\common\Gen1**.<br>2. Rename the Gen1 folder, then try again to install Security Manager Client.<br><br>If Gen1 is not present, rename **common** instead. |

| Message | Reason for Message | User Action |
|---|---|---|
| Error - Cannot Connect to Server<br>The client cannot connect to the server. This can be caused by one of the following reasons:<br>The server name is incorrect.<br>The protocol (http, https) is incorrect.<br>The server is not running.<br>Network access issues. Please confirm that the server name and protocol are correct.<br>The server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser. | Most likely, the server is misconfigured for HTTPS traffic. | 1. From a browser, log in to the Cisco Security Management Suite desktop at **https://**<*server*>**/CSCOnm/servlet/login/login.jsp**.<br>2. Click **Server Administration**.<br>3. In the Admin window, select **Server > Security**.<br>4. From the TOC, select **Single Server Management > Browser-Server Security Mode Setup**, then confirm that the Enable radio button is selected.<br>If the radio button is not selected, select it now, then click **Apply**.<br>1. When prompted, restart the Cisco Security Manager Daemon Manager.<br>2. Wait 5 minutes, then try again to use Security Manager Client.<br>If you still cannot connect, consider the other possible problems that the error message describes. |
| Error - Cisco Security Agent Running<br>Installation cannot proceed while the Cisco Security Agent is running<br><br>Do you want to disable the Cisco Security Agent and continue with the installation? | Cisco Security Agent needs to be stopped during the client installation. | • Click **Yes** to disable the Cisco Security Agent.<br>• Click **No** to cancel the operation and stop the Cisco Security Agent manually.<br>• Click **Help** to access online help for Security Manager client. |
| Error - Cisco Security Agent not Stopped<br>The installation will be aborted because the Cisco Security Agent could not be stopped.<br>Please attempt to disable Cisco Security Agent before repeating the installation process. | Security Manager client was unable to stop the Cisco Security Agent. | Click **OK** to close this error message and abort the installation. Manually disable the Cisco Security Agent before retrying the installation. |
| Error occurred during the installation: null. | Previous software installations and uninstallations caused InstallShield to run incorrectly. | 1. Navigate to C:\Program Files (x86)\Common Files\InstallShield\Universal\common\Gen1.<br>2. Rename the Gen1 folder, then try again to install Security Manager Client.<br>If Gen1 is not present, rename **common** instead. |

| Message | Reason for Message | User Action |
|---|---|---|
| `Errors occurred during the installation.`<br>• null | 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. |
| `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 2008, its Internet Explorer Enhanced Security default settings might stop you from downloading the client software installation utility from your server. | 1. Select **Start > Control Panel > Add or Remove Programs**.<br>2. Click **Add/Remove Windows Components**.<br>3. When the Windows Component Wizard window opens, uncheck the **Internet Explorer Enhanced Security Configuration** check box, click **Next**, then click **Finish**. |
| `Please read the information below.`<br><br>`The following errors were generated:`<br>• WARNING: The < *drive* > partition has insufficient space to install the items selected. | You tried to install Security Manager Client on a drive or partition that does not have enough free space. | Click **Back**, then select a different location in which to install Security Manager Client. |
| `Unable to Get Data`<br>`A database failure prevented successful completion of this operation.` | 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 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.

**Q.** The installer says that a previous version of the client is installed and that it will be uninstalled. However, I do not have a previous version of the client installed. Is this a problem?

**A.**During installation or re-installation 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, use the Registry Editor to delete the following key to prevent this message from being displayed during subsequent installations:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client. (To open the Registry Editor, select **Start > Run** and enter **regedit**.) Also, rename the C:\Program Files (x86)\Zero G Registry\.com.zerog.registry.xml file (any name will do).

# Client Problems After Installation

**Q.**Why does the interface not look right?

**A.** An older video (graphics) card might fail to display the Security Manager GUI correctly until you upgrade its driver software. To test whether this problem might affect your client system, right-click **My Computer**, select **Properties**, select **Hardware**, click **Device Manager**, then expand the **Display adapters** entry. Double-click the entry for your adapter to learn what driver version it uses. You can then do one of the following:

- If your client system uses an ATI MOBILITY FireGL video card, you might have to obtain a video driver other than the driver that came with your card. The driver that you use must be one that allows you to configure Direct 3D settings manually. Any driver lacking that capability might stop your client system from displaying elements in the Security Manager GUI.
- For any video card, go to the web sites of the PC manufacturer and the card manufacturer to check for incompatibilities with the display of modern Java2 graphics libraries. In most cases where a known incompatibility exists, at least one of the two manufacturers provides a method for obtaining and installing a compatible driver.

**Q.** Why is the 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.** Why is the Security Manager Client missing from the Start menu for some or all the users on a workstation on which it is installed?

**A.**When you install the client, you select whether shortcuts will be created for just the user installing the product, for all users, or for no users. If you want to change your election after installation, you can do so manually by copying the Cisco Security Manager Client folder from Documents and Settings\<user>\Start Menu\Programs\Cisco Security Manager to Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager. If you elected to not create shortcuts, you need to manually create the shortcut in the indicated All Users folder.

**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.)

**Note** You might have to create an entry for your DNS additional entry which will point to the same IP address (which will be used in the Security Manager client application's “Server Name” field) in the httpd.conf configuration file under *NMSROOT~/MDC/Apache/conf/* and restart the Daemon Manager. Such an entry can help you establish connections to your server. Examples: ServerName , foo.example.com . [**Tip**: The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.]**

**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 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...?

| | |
|---|---|
| ... | Verify that your server meets the minimum hardware and software requirements. See Server Requirements and Recommendations. |
| | There are two possible explanations:<br>• 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.<br>• 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 *NMSROOT* \lib\classpath subdirectory on your server, where *NMSROOT* is the directory in which you installed Common Services (the default is C:\Program Files (x86)\CSCOpx):<br>1. Either contact Cisco TAC for assistance in replacing **comUser.dat** or re-install Security Manager.<br>2. Create a Common Services password that does not use special characters. |

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:

- 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

Wait 5 minutes, then try again to start Security Manager Client.

**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

**Q.** How can I clear the server list from the Server Name field in the Login window?

**A.**Edit csmserver.txt to remove unwanted entries. The file is in the directory in which you installed the Security Manager client. The default location is C:\Program Files (x86)\Cisco Systems\Cisco Security Manager Client.

**Q.** The Security Manager client 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 (x86)\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:

- After you log in to the server using a browser, 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. If the setting is Disabled, use HTTP.
- When logging in using the client, first try HTTPS mode (check the HTTPS checkbox). If you get the message “Login URL access is forbidden; Please make sure your protocol (HTTP, HTTPS) is correct,” the server is probably running in HTTP mode. Uncheck the HTTPS checkbox and try again.

**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 (x86)\Cisco Systems\Cisco Security Manager Client\jars, modify the DEBUG_LEVEL parameters to include DEBUG_LEVEL=ALL and then restart the Security Manager client.

**Q.** 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. Can I fix this?

**A.**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.

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.

**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 .

# 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.

**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

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. 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.

**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 > Debug Options**, then check the **Capture Discovery/Deployment Debugging Snapshots to File** 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. You should change debugging levels only if the Cisco Technical Assistance Center (TAC) asks you to change them.

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

| From a Security Manager client system: | From a Security Manager server: |
|---|---|
| 1. After you establish a Security Manager Client session to your server, click **Tools > Security Manager Diagnostics**, then click **OK**.<br><br>The CSMDiagnostics.zip file is saved on your server in the *NMSROOT* \MDC\etc\ directory, where *NMSROOT* is the directory in which you installed Common Services (C:\Program Files (x86)\CSCOpx, for example).<br><br>1. Click **Close**.<br><br>**Note** We recommend that you rename this file so it does not get overwritten each time you run this utility. | 1. Open a Windows command window, for example, by selecting **Start > Run**, then enter **command**.<br><br>2. Enter **C:\Program Files (x86)\CSCOpx\MDC\bin\CSMDiagnostics**. Alternatively, to save the ZIP file in a different location than *NMSROOT* \MDC\etc\, 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 , on page 28.

**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 **Cisco_Prime_install_*.log**.

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....
```

You can check the errors for uninstall log same as for the install log.

Use a text editor to open **Cisco_Prime_uninstall_*.log**.

# Symantec Co-existence Issues

If you are using Symantec Antivirus Corporate Edition 10.1.5.5000 and Security Manager on the same system and observe any issues during Security Manager startup, follow this procedure:

**Procedure**

**Step 1** Disable Symantec Antivirus services completely.

**Step 2** Restart Security Manager services. (See Restarting All Processes on Your Server , on page 28.)

**Step 3** Restart the set of Symantec services (Symantec Antivirus, Symantec Antivirus Definition Watcher, Symantec Settings Manager, and Symantec Event Manager) in such a way that Symantec Event Manager is started last.

# Problems after Installing Windows Updates

Problems can occur with the Security Manager Daemon Manager after installing Microsoft Windows updates. The reason is that installing Windows updates may update *.dll files that affect the functionality of Common Services and other applications that depend on them.

This problem can be recognized by the following symptoms: After a Windows update, Security Manager will start all processes; however, Security Manager will be unreachable over HTTPS and therefore from the Security Manager client, which uses HTTPS.

This problem occurs because Common Services relies on files and associations within Windows. These files can be altered to correct vulnerabilities and protect Windows from exploits. However, as an unintended side effect, these changes can cause the Security Manager server to act abnormally when it is restarted.

This problem can occur any time that Windows Update, or any other application, makes changes to Windows that affect *.dll files, executables, startup processes, Windows components, or partition sizes.

To resolve this problem in cases where changes in Windows have been made and Security Manager acts abnormally when it is restarted, Security Manager must be re-installed.

Ensure that you back up your Security Manager server before running Windows Update or any other installer package.

# Backup of Cisco Security Manager Server

Cisco recommends you to backup Security Manager server regularly. In particular, if regular backups have not been made, or if many changes have been made to your Security Manager installation, you should backup your Security Manager server.

**Problem** When you backup, either manual or scheduled, it may fail to be completed. This failure may be caused due to "INFO: File not exists.SQL " or validation failure.

**Solution** Attach the dbbackup_timestamp.log and raise a Tac case.

# Problem Connecting to an ASA Device with Higher Encryption

This troubleshooting topic may help you if you are unable to add and discover an ASA device with higher encryption. In particular, if you want to use AES-282, you must download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. Security Manager does not include this extension, but it does support it.

**Problem** The problem occurs when the certificate contains a key longer than 1024 bits. The cryptography strength limitations placed by the default policy files included with Java Runtime Environment (JRE) give the highest strength cryptography algorithms and key lengths which are allowed for import to all countries.

**Solution** If your country does not place restrictions on the import of cryptography, you can download the unlimited strength policy files:

**Step 1** Go to http:// java.sun.com/javase/downloads/index.jsp.

**Step 2** Download the “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.”

**Step 3** Follow the instructions in the README.txt file in the downloaded package.

# Pop-up Showing Activation.jar in Use During the Time of Installation

This troubleshooting topic may help you if, during installation, a pop-up window appears with the message "Activation.jar being used by some other service."

**Tip** This problem is extremely rare.

**Before You Begin**

Any anti-virus or monitoring agent process in the server should be shut down before the installation. For more information, refer to Readiness Checklist for Installation.

**Problem**

A pop-up window appears with the message "Activation.jar being used by some other service."

**Solution**

Use the following procedure.

**Step 1** Click OK on the pop-up and complete the installation.
**Step 2** Uninstall Security Manager and restart the server.
**Step 3** Install Security Manager again.
**Step 4** Immediately after the start of the installation, enter "services.msc" at a command prompt and press Enter.
**Step 5** When the Services menu opens, keep refreshing it until "Cisco Security Manager Daemon Manager" appears.
**Step 6** Right-click CSM Daemon Manager > Properties > Startup type and then click Disabled.
**Step 7** Right-click CWCS syslog service > Properties > Startup type and click Disabled.
**Step 8** After the installation is complete, and at the time of server restart, change the startup type of both of the above services from "Disabled" to "Automatic" mode.

# How to Set the Locale for the Windows Default User Template to U.S. English

If you normally use a non-U.S. English Windows locale, you must change the default system locale to U.S. English before installing Security Manager; changing the default system locale and rebooting the server does not change the default profile. It is not sufficient for the current user only to have the proper settings; this is because Security Manager creates a new account ("casuser") that runs all Security Manager server processes.

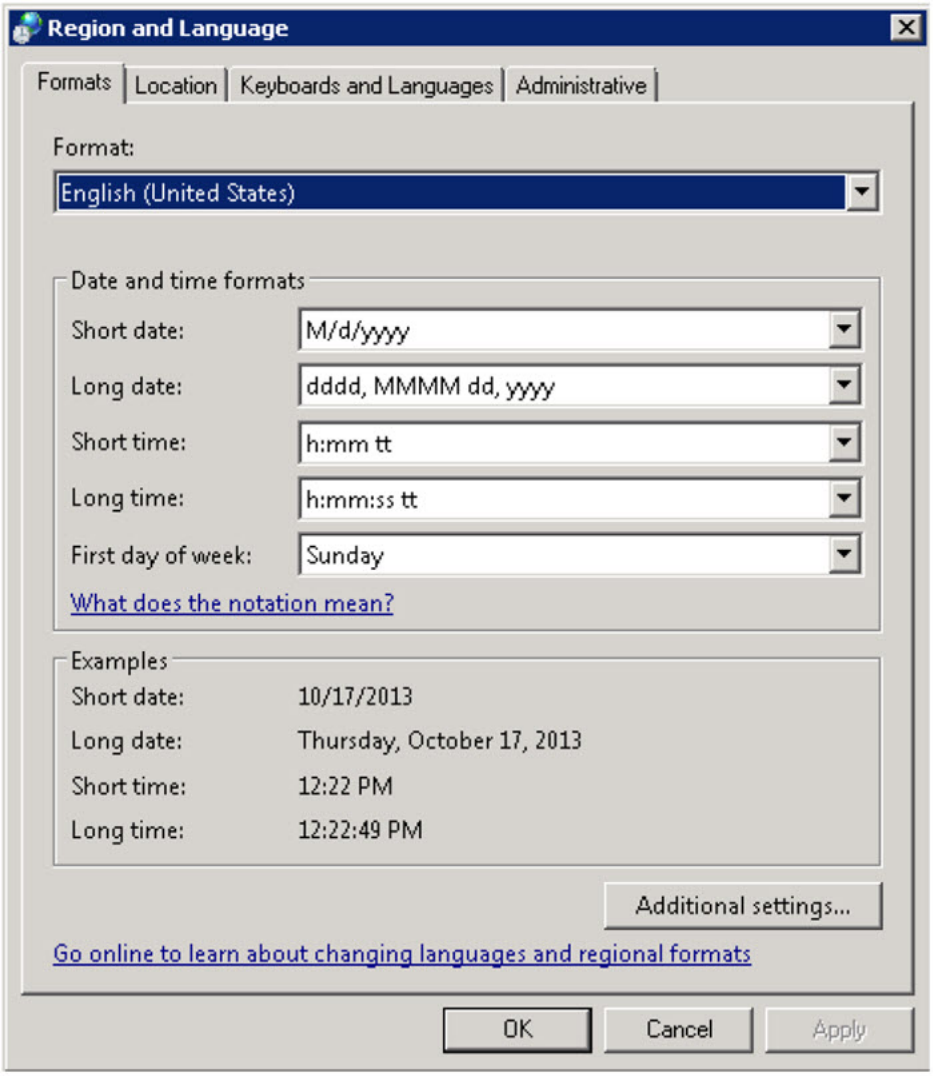
This section explains how to configure region and language settings on the Security Manager server, especially if you normally use a non-U.S. English Windows locale. The specific details apply to Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit, but they are very similar for the other supported server operating systems, namely the following ones:

- Microsoft Windows Server 2019 Standard—64-bit
- Microsoft Windows Server 2019 Datacenter—64-bit
- Microsoft Windows Server 2012 Standard—64-bit
- Microsoft Windows Server 2012 Datacenter—64-bit

To ensure that all newly created users have the same settings as the current user, you need to copy the settings for the current user to new user accounts. This can be done as shown below.

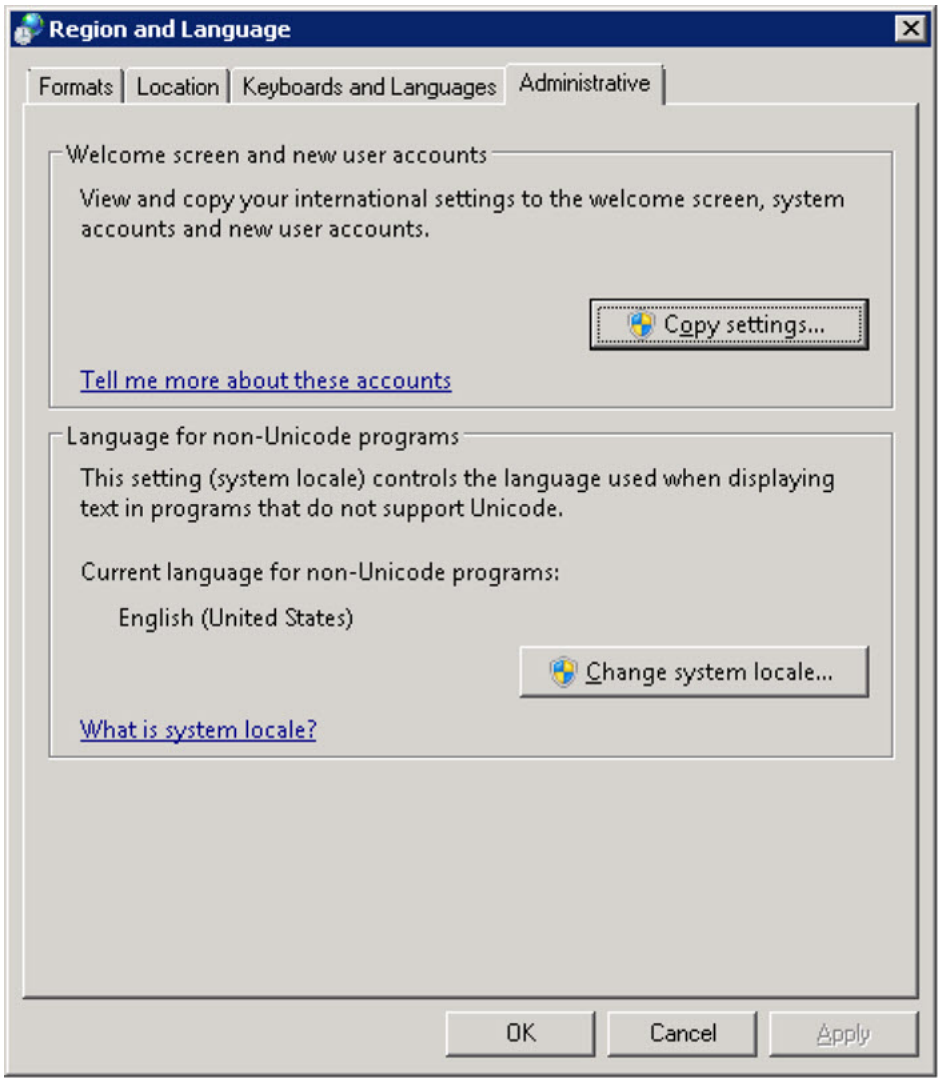
Ensure that the current user has proper U.S. English locale settingsin the Region and Language dialog box. (The navigation path to this dialog box is Start > Control Panel > Region and Language.)

Figure A-1 **Windows Region and Language dialog box**




Click the **Administrative** tab. Find the **Copy Settings...** button.

Figure A-2 **Administrative tab**




Click the **Copy settings...** button. The Welcome screen and new user account settings dialog box will appear.

Under “Copy your current settings to:” check the “New user accounts” box. This will ensure that all newly created users have the same configuration as the current settings.

Finally, install (or re-install) Cisco Security Manager server. In the new installation, the new account (“casuser”) that runs all Security Manager server processes will have a U.S. English default profile.

# How to disable the RMI Registry Port

In a typical Cisco Security Manager configuration the RMI registry port is open by default. You may need to disable this in a typical Cisco Security Manager configuration. Follow the steps below, to disable the RMI Registry Port:

**Problem**

Disable the RMI Registry Port

### Solution

Use the following procedure.

**Step 1** Stop Cisco Security Manager Server.

**Step 2** Export the ESS registry entry from the following Windows registry path in Cisco Security Manager Server.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager\CurrentVersion\Daemons\ESS

**Note** This is recommended, to create a backup.

**Step 3** Run the **ESS_Reg_Edit.bat** file. This file is available in Bug Search Kit (Attached in the defect CSCvc21327). The file will update the ESS registry entry by removing the JMX remote monitoring parameter in the Arguments Key.

**Step 4** Locate the **activemq.xml** file at this location ~CSCOpx\objects\ess\conf\activemq.xml

**Step 5** Modify the "createConnector" value as false as follows:

<managementContext>

<managementContext createConnector="false"/>

</managementContext>

**Step 6** Save **activemq.xml**.

**Step 7** Restart Cisco Security Manager.