Cisco Software Manager User Guide

This document describes how to install and configure the Cisco Software Manager that eases the Software Maintenance Upgrades (SMUs) management process on devices running the Cisco IOS XR Software.

Introduction

The Cisco Software Manager (CSM) provides SMUs recommendations to users and reduces their effort in manually searching, identifying, and analyzing SMUs that are needed for a device. To provide the recommendations, CSM must be connected through the Internet to the cisco.com domain. The CSM can connect to multiple devices and provide SMUs management for multiple Cisco IOS XR platforms and releases.

The Cisco Software Manager (CSM) is a standalone Java application that can be installed on Windows, MAC, and UNIX. The CSM supports Cisco CRS and Cisco ASR 9000 devices.

Installing the Cisco Software Manager

This section explains the computer requirements, pre-requisites, and software installation procedure on Windows, MAC, and UNIX.

To download the Cisco Software Manager (CSM), click CSM.

Computer Requirements

The following section lists the computer requirements:

Area	Requirements	Notes
Operating System	• PC: Windows • Unix • Apple Mac OS X	Use the latest patch/Service Pack released by the OS vendor. Check with the vendor for the latest patch/Service Pack.
Java Runtime Environment	• JRE 1.6 • JRE 1.7	To download JRE, click this URL.

Pre-Requisites for Installing the Cisco Software Manager

The installation script (SetupCSM.cmd for Windows or SetupCSM.sh for Unix and MAC) requires JRE to be in the search path. If JRE is not present in the search path, users can invoke the installer using the direct path. For information, see Installing on Windows, on page 3, Installing on MAC, on page 3, or Installing on UNIX, on page 4.

This section contains steps to include JRE in the search path on Windows system:

Procedure

Step 1 Go to **Control Panel>System>Advanced System Settings**.

Step 2 In the System Properties window, click **Environment Variables**.

Step 3 In the System Variables section, select **Path** and click **Edit**.

Step 4 Append *C:\Program Files\java\jre6\bin* to the **Variable value** field.

Step 5 Click **OK**. JRE is included in the search path.

Installing on Windows

Procedure

Step 1 From cisco.com, download the file, CSM-1.0.zip.

Step 2 Unzip the file, CSM-1.0.zip.

Step 3 Double-click the file, SetupCSM.cmd. Cisco Software Manager begins to install.
A shortcut that launches CSM software is created on the desktop.

Note The SetupCSM.cmd script assumes java to be in the search path. If that is not the case, users must include java in the search path and double-click SetupCSM.cmd, or execute "<*JREDir*>\bin\java -jar installer.jar" in the command prompt. *JREDir* is the location at which JRE is present, which is C:\Program Files (x86)\java\jre6 for Windows 7 and C:\Program Files\java\jre6 for Windows XP.

Step 4 Double-click the CSM icon at the desktop to launch the CSM software.

Installing on MAC

Procedure

Step 1 From cisco.com, download the file, CSM-1.0.zip at your desktop.

Step 2 Double-click the file, CSM-1.0.zip, to unzip. The CSM-1.0 folder is created.

Step 3 Open a terminal window and change to the directory to where you extracted the zip file.

Example:
cd/Users/<username>/Desktop/CSM-1.0.

Step 4 Execute the following commands on the terminal window to run the installation script.

- chmod 777 SetupCSM.sh
- ./SetupCSM.sh

Cisco Software Manager begins to install. A shortcut that launches CSM software is created on the desktop.

Note The SetupCSM.sh script assumes java to be in the search path. If that is not the case, you can invoke java (JVM) directly using the full path: /usr/bin/java -jar installer.jar.

Step 5 Double-click the CSM icon at the desktop to launch the CSM software.

Installing on UNIX

Procedure

Step 1 From cisco.com, download the file, CSM-1.0.zip.

Step 2 Open a terminal window and do the following:

a) Create a new folder.

Example:
mkdir newfolder

b) Unzip the file, CSM-1.0.zip, at the newly created folder.

Example:
unzip CSM-1.0.zip

c) Change to the directory to where you extracted the zip file.

d) Run the installation script:

- chmod 777 SetupCSM.sh
- ./SetupCSM.sh

Cisco Software Manager begins to install.

Note The SetupCSM.sh script assumes java to be in the search path. If that is not the case, you can invoke java (JVM) directly using the full path: /usr/bin/java -jar installer.jar.

Step 3 To launch the CSM software, execute one of the following commands:

- /users/<username>/csm/bin/CSM1.0.cmd
- /users/<username>/CSM1.0

Icons and Names

The following table lists the icons and their names:

Icons	Names
	**Set Up**
	**Task**
	**Refresh**

Icons	Names
	**Import**
	**Add Network Elements**
	**Remove Network Elements**

Configure the Cisco Software Manager

After installing the Cisco Software Manager, users can configure the software to perform the following tasks:

1 Set Up Cisco Software Manager. See Set Up the Cisco Software Manager, on page 6.

2 Retrieve SMUs Information from Cisco.com. See Retrieve SMUs Information from Cisco.com, on page 6. After retrieving SMUs information from cisco.com, users can execute the following tasks:

- Create a Watch List
- Create TAR File
- View/Extract TAR File
- Export SMU Information

Note See Execute SMU Tasks, on page 7 to create a watch list or TAR file, view/extract TAR file, and to export SMU information.

3 Obtain SMUs Recommendations. See Obtain SMUs Recommendations, on page 8.

- Identify Superseded SMUs. See Identify Superseded SMUs, on page 15.
- Create and Assign Custom Suggested File. See Create and Assign Custom Suggested File, on page 15.
- Generate the Conformance report. See Generate the Conformance Report, on page 16.

- Create a Watch List
- Create TAR File
- View/Extract TAR File
- Export SMU Information

Note See Execute SMU Tasks, on page 7 to create a watch list or TAR file, view/extract TAR file, and to export SMU information.

4 Obtain an Optimized SMU List. See Obtain an Optimized SMU List, on page 16.

Set Up the Cisco Software Manager

Procedure

Step 1 Launch the CSM software and click the **Set Up** icon on the main tool bar.

Step 2 Define the following attributes in the Set Up dialog box:

- SMU Repository Directory—Specify the location on the system where the SMUs can be are stored. This is useful first to determine whether the SMU is present at that location or not, and accordingly the software displays an appropriate graphical icon next to the SMU entry. A tar file can be created only if the SMUs are present in this location.
- Polling Interval—Specify how often the CSM software must query cisco.com to retrieve SMU information. Before the query, the software first polls all the connected devices for an up-to-date package information.
- Email Notification Settings—Specify the email account where the email notification has to be sent when new SMUs are discovered. The Test Email Account Settings can be used to verify if the email delivery is operational.

Retrieve SMUs Information from Cisco.com

Based on the selection of the platform and release, the user can view the list of SMUs retrieved from cisco.com:

Procedure

Step 1 Launch the CSM Software.

Step 2 Click the **Platforms and Releases** button and select the desired platform and the release version. The SMUs details retrieved from cisco.com are displayed.

Note If the software fails to retrieve the information, a red highlight message will be displayed. You must close the Platforms and Releases tab and reopen the tab to reconnect to cisco.com. Click the **Open Tab** button and select **Platforms and Releases** to reopen the tab.

Step 3 Click the **Filter (Optimal)** button and choose an appropriate filter option:

- Select the **Optimal** filter option to view only optimal SMUs. This option excludes all superseded SMUs that are not a pre-requisite for other SMUs.
- Select the **ALL** filter option to view all SMUs.

By default, the Optimal filter option is enabled.

View SMU Details

- To view the details of a SMU, click that specific SMU row. A balloon tool tip that contains the SMU information (pre-requisites, superseded, and superseded by information) is displayed. To view the information of other related SMUs (pre-requisites, supersedes, and so on), click the SMU hyperlink. Use the blue arrow icons to navigate between different SMU details. You can annotate a SMU by entering the information in the annotation field at the bottom of the tool tip.
- To view the SMU DDTS information:
  - Click the DDTS hyperlink. The default browser is launched.
  - Enter the Cisco Authentication login details. The DDTS information from the Software Bug Toolkit web site is displayed.

Select SMUs

The checkbox on the table header is used to select or de-select all SMUs at once. If all the SMUs listed in the SMU table are not selected, the checkbox is displayed as a filled rectangle.

Execute SMU Tasks

The other actions that the users can perform after retrieving the SMUs from cisco.com are:

Create a Watch List— The Watch list allows the user to keep track of the new SMUs that might be released for a specific platform and release. The details of the new SMUs is provided by the Cisco escalation team to the customer/user. To create a watch list, do the following:

1. Click the **Task** icon and select **Watch List**.
2. Enter the SMU ID and click **Save**. An alert notification is displayed when the SMU entered in the watch list for is available, during the next query to cisco.com.

Create TAR File—The TAR file contains the SMUs that can be installed on the device:

1. Manually download the SMUs from cisco.com at your local system in the SMU repository directory.
2. Click the **Refresh** icon to update the status of the SMU entries. The SMUs that are stored in the SMU repository directory are indicated by a green check icon in the ST (status) column.

3 Select the SMUs with the green check icon and click the **Task** icon and select **Create TAR File**. The software alerts the user in case of any missing prerequisites.

View/Extract TAR File—Users can view the contents of a TAR file and selectively extract the desired SMUs. Click the **Task** icon and select **View/Extract TAR File** to perform this action.

Export SMU Information—Export SMU details of the selected SMUs or those SMUs that are not installed on the device to an HTML file, thus:

1 Click the **Task** icon and select **Export SMU Information**.

2 Select the export option. The SMU information is saved in the HTML file.

The SMU details are sorted by the SMU posted date. Any annotation entered for a SMU will be present in the Comments column of the HTML file.

Obtain SMUs Recommendations

To obtain SMUs recommendations for a specific platform and release, users must provide the device package information to the CSM software for that particular platform and release using one of the three sources:

- CLI Output (show install active summary) , on page 8
- Import File, on page 9
- Connected Device, on page 9

The CSM software processes the information that is provided using one of the sources above and displays the SMUs recommendations in the Software Monitor pane. For SMU Monitor pane details, see SMU Monitor Pane, on page 14.

CLI Output (show install active summary)

The users can provide the CLI Output (show install active summary) information to the CSM software using the CLI Source tab.

Procedure

Step 1 Launch the CSM software.

Step 2 Click the **Open Tab** button on the main tool bar and select **CLI Source**. The CLI Source tab is displayed.

Step 3 Enter the device name and copy-paste a complete 'show install active summary' CLI output.

Step 4 Click **Next**. The SMU Monitor Pane, on page 14 is displayed. The name of the SMU Monitor pane indicates the input source, platform, and release number.
Whenever the software discovers new SMUs from cisco.com, an alert message is displayed.

Import File

The CLI Source tab is used to provide the “show install active summary” information for only one device. To provide package and SMU information of multiple devices at the same time, an external file that contains these details can be imported to the CSM software. To import an external text file, do the following:

Procedure

Step 1 Click the **Import** icon on the main tool bar.

Step 2 Browse to select the external file and click **Import**. The external file must follow the expected format as outlined in the Import dialog box.
Once the external file is imported, the devices whose package information was present in the external file appear as gray icons in the Network Elements pane.

Step 3 Click each device in the Network Elements pane to view the results in the SMU Monitor Pane, on page 14.

Connected Device

To provide package information through a connected device to the software, connectivity must be established between the device and the computer that hosts the software. Before connecting the device to the software, users must:

1. Verify device requirements. See Device Requirements, on page 10.
2. Verify mandatory configuration on the device for the required connection type. See Supported Connection Types, on page 10.
3. Create Login profiles. See Creating Login Profiles, on page 10.

Once the above listed conditions are met, the users can login to the device. See Login to Device, on page 11.

When the software is successfully connected to the device, it retrieves the package information and adds the connected device into the Network Elements tree pane. Devices with the same platform and release are grouped under the same sub-tree (for example, ASR9K-PX-4.2.3). Click each device in the Network Elements pane to view their results in the SMU Monitor pane. The Package table will be updated based on the selection made. For SMU Monitor pane details, see SMU Monitor Pane, on page 14.

A connected device displayed in the Network Elements pane can have two colors—orange or blue. Orange indicates failure in establishing connection between the software and the device during the next polling. Blue indicates successful connection between the software and the device.

Note If the device is in the discovering state for a long time, the user must remove the device using the **Remove Network Element** icon and ensure **xml agent tty** is configured on the device and then login to the device again.

Supported Connection Types

The following table lists the connection types that Cisco Software Manager supports to establish connectivity to the device and the mandatory configuration required on the device:

Connection	Mandatory Router Configuration
Telnet	telnet vrf default ipv4 server max-servers 20
SSHv1	ssh server hostname <*hostname*> domain name <*domain*>
SSHv2	ssh server v2

Note Install crypto key on the router when the sshv1 or sshv2 connection is used.

Device Requirements

The following section lists the requirements for Cisco CRS and Cisco ASR 9000 routers to establish connectivity with the CSM software:

- Install manageability PIE:
  - (Cisco ASR9K) asr9k-mgbl-p.pie must be loaded
  - (Cisco ASR9K) asr9k-k9sec-p.pie must be loaded for SSHv1 and SSHv2
  - (Cisco CRS) hfr-mgbl-px.pie must be loaded
  - (Cisco CRS) hfr-k9sec-px.pie must be loaded for SSHv1 and SSHv2
- Enable the XML agent**— xml agent tty** must be configured on the device.

Creating Login Profiles

Users can create login profiles and save the login information in an XML file. During the next consecutive logins, the software uses the information present in this XML file and allows the user to login without the need to re-enter the login details again. The XML file (LoginInformation.xml) created is stored at the application directory (**...\csm\versions\1.0**) and can be shared with other users.

To create the login profile, do the following:

Procedure

Step 1 Launch the CSM software.

Step 2 Click the **Add Network Elements** icon on the main tool bar. The Login dialog box is displayed.

Step 3 Right-click **Login Information** and choose either **Add New Device Group** or **Add New Device**. **Add New Device Group** creates a device group to which devices can be added later and **Add New Device** adds a device.
The attributes present in the Add New Device dialog box are explained below:

- Connection Category—Choose **IP** if there is direct connectivity between the computer which hosts the software and the device, else choose **Scripted**.
- Connection Type —Choose any one of the listed connection types: **Telnet/SSHv1/SSHv2**
- Device IP/Name—(Only **IP** connection category) Enter the device management IP address or the Host Name.
- Node Name/Port—(Only **Scripted** connection category) Enter the intermediate server name or IP address. Enter the port number if the server does not use the default Tenet/SSH port number. Click "…" to add additional script information. For more information on entering details in this field, refer to the Login Script Steps, on page 12.
- Device Description—Description of the device.

Login to Device

To login to the device, do the following

Procedure

Step 1 Launch the CSM software.

Step 2 Click the **Add Network Elements** icon on the main tool bar.

Step 3 Select the device and enter the login credentials that are defined for the device. See Direct Login and Scripted Login to the Device, on page 11.

Note Users can log into multiple devices simultaneously if they share the same user name and password. To do so, select multiple devices by using the **<Ctrl>** / **<Shift>** key or select the entire device group.

Direct Login and Scripted Login to the Device

Connection between the computer that hosts the software and the device can be established in two ways:

- Direct Connection or Direct Login—The computer that hosts the software is directly connected to the device. In this case, choose **IP** as the Connection Category in the Login Screen.

- Indirect Connection or Scripted Login—The computer that hosts the software is connected to the device through an intermediate server. In this case, choose **Scripted** as the Connection Category in the Login screen.

The attributes in the Login screen vary depending on the choice of Connection Category (**IP** or **Scripted**).

Direct Login

When **IP** is chosen as the Connection Category, the following attributes are displayed on the Login screen:

- Device User Name—Enter the device user name
- Device Password—Enter the device password
- Connection Type—Choose Telnet, SSHv1, or SSHv2
- Device IP/Name—Enter the device management IP address.

Scripted Login

When **Scripted** is chosen as the Connection Category, the following attributes are displayed on the Login screen:

- Scripted User Name—Enter the intermediate server username
- Scripted Password—Enter the intermediate server password
- Device User Name—Enter the device user name
- Device Password—Enter the device password
- Connection Type—Choose Telnet, SSHv1, or SSHv2
- Node Name/Port—Enter the intermediate server name or IP. Choose "..." to add additional script information. Enter the port number if the server does not use the default Tenet/SSH port number. For more information, see Login Script Steps, on page 12 .
- Device Description—Enter the device description.

Login Script Steps

Based on the connection type (telnet, sshv1, or sshv2) between the computer that hosts the software and the intermediate server, and the connection type between the intermediate server and the device, the following section provides examples of entering additional script information in the **Login Script Steps** dialog box, while creating a login profile or while logging into the device. Click **"...."** to enter the details in the **Login Script Steps** dialog box while creating a login profile or while logging into the device. The steps outlined in the **Login Script Steps** depict the manual login sequence:

- The “Wait For” data fields contain prompted string returned by the intermediate server.
- When CSM sees the “Wait For” string, it responds by sending the data defined in the “Send” data field.
- Scripted Username and Scripted Password are the intermediate server authentication that can be selected from the drop down. During the actual login, these credentials must be entered by the user in the login screen.

- The appearance of the Login prompt (**login:**) may vary depending on the system (Windows, MAC, or UNIX) where the CSM software was installed.

  Telnet —>Telnet scripted login indicates that the connectivity type between the computer that hosts the software and the intermediate server is Telnet and the connectivity type between the intermediate server and the device is Telnet.

Table 1: Telnet —>Telnet Scripted Login

Wait For:	**login:**	Send:	**Scripted Username**
Wait For:	**Password:**	Send:	**Scripted Password**
Wait For:	*intermediate server prompt*	Send:	telnet <*device host name or ip address*>

Telnet —>SSH scripted login indicates that the connectivity type between the computer that hosts the software and the intermediate server is Telnet and the connectivity type between the intermediate server and the device is SSH.

Table 2: Telnet —>SSH Scripted Login

Wait For:	**login:**	Send:	**Scripted Username**
Wait For:	*intermediate server prompt*	Send:	ssh -l <*device username*> <*device password*>
Wait For:	**password:**	Send:	<*device password*>

SSH—>Telnet scripted login indicates that the connectivity type between the computer that hosts the software and the intermediate server is SSH and the connectivity type between the intermediate server and the device is Telnet.

Table 3: SSH —>Telnet Scripted Login

Wait For:	**login:**	Send:	**Scripted Username**
Wait For:	*intermediate server prompt*	Send:	telnet <*device host name or ip address*>

SSH —>SSH scripted login indicates that the connectivity type between the computer that hosts the software and the intermediate server is SSH and the connectivity type between the intermediate server and the device is SSH.

Table 4: SSH —>SSH Scripted Login

Wait For:	**login:**	Send:	**Scripted Username**

Wait For:	*intermediate server prompt*	Send:	ssh -l *<device username>* *<device password>*
Wait For:	**password:**	Send:	*<device password>*

SMU Monitor Pane

The SMU Monitor pane contains two tables:

- **SMU Table—**Displays SMU information retrieved from cisco.com for a specific platform and release in the top window. SMUs that are already installed on the device are highlighted in green. SMUs that are not applicable to the device are highlighted in gray. For example, a SMU may require the mpls pie which is not installed on the device. By default, the software uses the Optimal filter option to display SMU entries in the SMU table. However, the user may select the All filter option to display all SMUs.
- **Package Table—**Displays the packages and SMUs that are currently present on the device in the bottom window. By default, the package table displays all the active packages (pies and SMUs). To display just the SMUs on the device, click the **SMUs Only** radio button. The package pie or SMU is highlighted in orange if it is in active, but not committed state (applicable only to connected devices).

The SMU and the Package tables have the quick search filter. The filter accepts a string pattern and filters the display list accordingly. The filter can be used to look up for a specific DDTS or SMUs within a specific functional area, for example, BGP. Turn off the filter if you suspect the SMU list on the SMU table should have more entries. Click the cross icon in the filter to turn off the filter.

The SMU Monitor pane automatically refreshes at every polling interval configured in the Setup dialog box. Also, users can manually refresh the SMU Monitor pane by clicking the **Refresh** icon to retrieve the updated SMU information from cisco.com. A manual refresh does not poll the latest package information from the device. To manually poll the device, use the **Refresh** icon on the Network Elements pane.

After obtaining the SMU recommendation from cisco.com, users can perform the following tasks:

- Identify Superseded SMUs, on page 15
- Create and Assign Custom Suggested File, on page 15
- Generate the Conformance Report, on page 16
- Create a Watch List.
- Create TAR File
- View/Extract TAR File
- Export SMU Information

Note See Execute SMU Tasks, on page 7 to create a watch list or TAR file, view/extract TAR file, and to export SMU information.

Identify Superseded SMUs

Based on the SMUs selected in the SMU table, the software identifies if there are any superseded SMUs on the device and applies a strikethrough font on the SMU names in the package table. The superseded SMUs can be removed and deactivated once the selected SMUs are activated. When the user clicks on the superseded SMU, a balloon tooltip is displayed with information on which SMUs superseded the SMU.

In addition, if a SMU is superseded by existing SMUs on the device, it will also take on the strikethrough front. To identify which SMUs are superseded by existing SMUs on the device, uncheck all the SMU entries on the SMU table. The quickest way to uncheck all SMU entries is by unchecking the checkbox on the table column header.

Create and Assign Custom Suggested File

A pre-certified SMU list that is used to validate against all the devices/routers is referred to as Custom Suggested SMUs. The CSM software allows the users to create a file that contains the Custom Suggested SMUs. Also, the user can assign an already existing file (external text file) that contains the required SMUs to validate the device. The custom suggested file contains only the SMU names. Each line in the file contains a SMU name.

Procedure

Step 1 Launch the CSM software.

Step 2 Obtain SMU recommendation from the software using any one of the following sources:

- CLI Output (show install active summary) , on page 8.
- Import File, on page 9.
- Connected Device, on page 9.

The SMU recommendation is displayed on the SMU monitor pane.

Step 3 Select the required SMUs from the SMU table.

Step 4 Click the **Suggest** button and choose one of the following:

- **Create Suggest File—**The selected SMUs can be saved to an external text file. Once the file is created successfully, the software prompts whether the user wants to assign this file for validating the device. Click **Yes** to assign or **No** to quit the action.
- **Assign File to Suggest—** Browse for an external text file that contains the required SMUs. The SMU details are displayed in the Assign File to Suggest dialog box. The assignment is saved and assigned to this particular platform and release.

Step 5 Click the **Suggest** button and choose **Enable Suggest**. A green tick mark is displayed against Suggest. The SMU Monitor pane is refreshed and the new list of suggested SMUs is displayed in the top window (SMU table) and the bottom window (Package table) is refreshed accordingly.

Note By default, the **Suggest** button displays a red cross which indicates it is not enabled.

Generate the Conformance Report

The Conformance report contains information about the selected SMUs and their install statuses on the selected devices. To generate the conformance report, do the following:

Procedure

Step 1 Launch the CSM software.

Step 2 Obtain SMU recommendation from the software using any one of the following sources:

- CLI Output (show install active summary) , on page 8.
- Import File, on page 9.
- Connected Device, on page 9.

The SMU recommendation is displayed on the SMU monitor pane.

Step 3 Select the SMUs and click **Conformance Report** at the bottom right corner. The SMU conformance report for the selected SMUs is displayed.
The user can choose to copy the report to the system clipboard or save the report as a text file. The results in the report are tab delimited and can be pasted onto Microsoft Excel spreadsheet or other applications.

Note If there are multiple devices under the same platform and release sub-tree (on the Network Elements pane), the users can choose to run the Conformance report against the current device or selected devices.

Obtain an Optimized SMU List

The CSM software can provide an optimized SMU list by identifying missing pre-requisites and superseded SMUs. To obtain an optimized SMU list do the following:

Procedure

Step 1 Launch the CSM software.

Step 2 Click the **Open Tab** button on the main tool bar and select **Optimize List**. The Optimize List tab is displayed.

Step 3 Provide the master SMU list using any one of the two options listed below:

- Copy and paste the master SMU list and click **Optimize**.
- Click **Read from TAR** to supply the SMU list using a tar file and click **Optimize**. The optimized list of SMUs is obtained.

Once the list is optimized, the users can do the following:

- **View Pre-requisite—**Click the **Pre-requisites** button to view the pre-requisite relationships. The **Pre-requisites** button will be enabled only if there is any missing pre-requisite.
- **Copy the list—**Click the **Copy** button to copy the annotated list or the optimized list.

The Annotated list includes the tagging seen on the window.

The Optimized list includes all the missing pre-requisites and excludes all the superseded SMUs.

- **Create a Suggest File—**Click the **Suggest** button to use the optimized list for creating a Suggest file.

Uninstalling the Cisco Software Manager

This section explains how to uninstall the Cisco Software Manager:

- Windows—Navigate to the csm\uninstall folder and click CSM1.0_uninstall.cmd
  - On Windows XP, the CSM folder is located at "C:\Documents and Settings\<username>"
  - On Windows 7, the CSM folder is located at "C:\Users\<username>"
- MAC—Execute the **/Users/<username>/csm/uninstall/CSM1.0_uninstall.sh** command on the terminal window.
- UNIX—Execute the **rm –R csm** on the terminal window.