## Post-upgrade Tasks

- Post-upgrade Task Flow, on page 1

### Post-upgrade Task Flow

Perform the tasks in this list for all upgrade and migration methods.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch the Software Version, on page 3</td>
<td>If you did not switch versions immediately after completing the upgrade, do so now in order to complete the upgrade. Do not perform a backup until you have switched to the new software version. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Remove the Serial Port, on page 4</td>
<td>Remove the serial port that you added during the pre-upgrade tasks so that it does not impact VM performance. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Restart Extension Mobility, on page 4</td>
<td>If you deactivated Cisco extension mobility as part of the pre-upgrade tasks, you can now restart it.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Restart TFTP Services, on page 5</td>
<td>Use this procedure to restart TFTP services on Unified CM nodes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Reset TFTP Parameters, on page 5</td>
<td>Reset TFTP parameters that are changed during the upgrade process.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Restore Enterprise Parameters, on page 5</td>
<td>Restore any Enterprise Parameter settings on IM and Presence Service nodes that may have been overwritten during the upgrade process.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> Reset High and Low Watermarks, on page 6</td>
<td>Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces. You can skip this task for PCD migrations.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> Updating VMWare Tools, on page 6</td>
<td>You must update the VMware Tools after you complete the upgrade.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> Install Locales, on page 7</td>
<td>After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Perform this procedure for all nodes.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> Restore the Database Replication Timeout, on page 9</td>
<td>Use this procedure if you increased the database replication timeout value before you began the upgrade process. Perform this procedure on Unified Communications Manager nodes only.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> Verify the Registered Device Count, on page 9</td>
<td>Use this procedure to verify your endpoints and resources on Unified CM nodes after the upgrade is complete.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> Verify Assigned Users, on page 10</td>
<td>Use this procedure to verify the number of assigned users on Instant Messaging and Presence nodes after the upgrade is complete.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> Test Functionality, on page 10</td>
<td>Verify phone functions and features are working correctly after the upgrade.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> Upgrade RTMT, on page 11</td>
<td>If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> Manage TFTP Server Files, on page 12</td>
<td>Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Unified CM nodes.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> Set Up a Custom Log-On Message, on page 13</td>
<td>Optional. For Unified CM nodes only, upload a text file that contains a customized log-on message.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> Configure IPSec Policies, on page 13</td>
<td>If you are completing a PCD migration from Release 6.1(5), you must recreate your IPSec policies as they are not migrated to the new release.</td>
<td></td>
</tr>
</tbody>
</table>
### Switch the Software Version

When you perform a standard upgrade, the new software is installed as an inactive version. You can reboot to the new software during the upgrade process or you can switch to the new version later.

If you did not switch versions immediately after completing the upgrade, do so now. You must switch versions so that the upgrade is complete and all nodes in the cluster are updated. Do not perform a backup until you have switched to the new software version.

When you switch versions, the system restarts, and the inactive software becomes active. The system restart may take up to 15 minutes. When you perform this procedure both the active and inactive software versions are indicated.

⚠️ **Caution**

This procedure causes the system to restart and become temporarily out of service.

#### Before you begin

The software versions on Unified Communications Manager and Instant Messaging and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch Instant Messaging and Presence.

Review the information in **Understanding Version Switching**

#### Procedure

**Step 1**  
If you switch versions in a multinode deployment, you must switch the publisher node first.

**Step 2**  
Log in to the management software for the node that you are upgrading:
• If you are upgrading an Instant Messaging and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
• If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

| Step 3 | Select Settings > Version. |
| Step 4 | Verify the version of the active software and the inactive software. |
| Step 5 | Select Switch Versions to switch versions and restart the system. |

After you perform a switch version when you upgrade Unified Communications Manager, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

**Remove the Serial Port**

During the pre-upgrade tasks, you added a serial port to the virtual machine to capture the upgrade logs. After you have successfully upgraded the system, you must remove the serial port so that it does not impact the performance of the virtual machine.

**Procedure**

| Step 1 | Power off the virtual machine. |
| Step 2 | Edit the settings to remove the serial port. For information about how to edit the settings, see the VMWare documentation. |
| Step 3 | Power on the virtual machine and proceed with the post-upgrade tasks. |

**Restart Extension Mobility**

Upgrades from Release 9.x or earlier require you to stop Cisco extension mobility before you begin the upgrade process. If you deactivated Cisco extension mobility as part of your pre-upgrade tasks, use this procedure to restart the service on Unified Communications Manager nodes.

**Procedure**

| Step 1 | From Cisco Unified Serviceability, choose Tools > Service Activation. |
| Step 2 | From the Server list, choose the node on which you want to deactivate services and click Go. |
| Step 3 | Select the Cisco Extension Mobility services. |
| Step 4 | Click Restart. |
Restart TFTP Services

Use this procedure to restart TFTP services on Unified Communications Manager nodes after you complete an upgrade.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified Serviceability, choose <strong>Tools &gt; Service Activation</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the <strong>Server</strong> list, choose the node on which you want to deactivate services and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the <strong>Cisco TFTP</strong> services.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

Reset TFTP Parameters

During the upgrade process, the TFTP service parameter **Maximum Serving Count** is changed to allow for an increased number of device registration requests. Use this procedure to reset the parameter after the upgrade is complete.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Cisco Unified CM Administration interface, choose <strong>System &gt; Service Parameters</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the <strong>Server</strong> drop-down list, select the node that is running the TFTP service.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the <strong>Service</strong> drop-down list, select <strong>Cisco TFTP service</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Advanced</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Set the <strong>Maximum Serving Count</strong> to the same value that you used prior to the upgrade, or to the value that is recommended for your configuration.</td>
</tr>
</tbody>
</table>

The default value is 500. We recommend that you use the default value if you run the TFTP service with other Cisco CallManager services on the same server. For a dedicated TFTP server, use the following values:

- 1500 for a single-processor system
- 3000 for a dual-processor system
- 3500 for dedicated TFTP servers with higher CPU configurations

Restore Enterprise Parameters

Some Enterprise Parameters exist on both Unified Communications Manager nodes and Instant Messaging and Presence nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on Instant Messaging and Presence nodes.
during an upgrade. Enterprise Parameters that are unique to Instant Messaging and Presence nodes are retained during an upgrade.

Use this procedure to reconfigure the settings on Instant Messaging and Presence nodes that have been overwritten during the upgrade process.

**Before you begin**

Make sure you have access to the settings that you recorded as part of the pre-upgrade tasks.

**Procedure**

**Reset High and Low Watermarks**

Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces.

**Procedure**

**Updating VMware Tools**

VMware Tools are a set of utilities for management and performance optimization. Your system uses one of the following VMware Tools:

- Native VMware Tools (provided by VMware)
- Open VMware Tools (provided by Cisco)
- To upgrade Unified Communications Manager from a version earlier than Release 11.5(x), you must use the native VMware tools option. You can change to open VMware Tools after the upgrade.

- For upgrades from Unified Communications Manager Release 11.5(1) onwards (for example, to a higher SU), you can choose whether your system use Native VMware or Open VMware Tools.

- For fresh installation and PCD migrations from Unified Communications Manager Release 11.5(1) onwards, open VMware tools installed by default.

**Procedure**

**Step 1**
Execute a command `utils vmtools status` to ensure that VMware tools are currently running.

**Step 2**
If necessary, run one of the following commands to switch to the desired VMware tools platform: `utils vmtools switch native` or `utils vmtools switch open`.

**Step 3**
Follow one of the methods below if you are using *Native VMware Tools*:

- Initiate the automatic tools update with the viClient.

  **Note** For ESXI 6.5 VM tools update, power off the VM before updating the configuration parameters. Choose the Edit settings > options > Advanced > General > Configuration parameters and then add:

  ```
  tools.hint.imageName=linux.iso
  ```

  • Configure the tool to automatically check the version during a VM power-on and upgrade.

  For information about how to configure these options, refer to VMware documentation. You can also find more information by searching the topic "VMware Tools" at [https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html#vmtools](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html#vmtools).

**Install Locales**

Use this procedure to install locales. After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Install the latest version of the locales that match the major.minor version number of your Unified Communications Manager node or Instant Messaging and Presence node.

You can install locales on Unified Communications Manager or on Instant Messaging and Presence nodes. If you are installing a locale for both products, install the locale on all cluster nodes in the following order:

1. Unified Communications Manager publisher node
2. Unified Communications Manager subscriber nodes
3. IM and Presence database publisher node
4. IM and Presence subscriber nodes

If you want to install specific locales on IM and Presence Service nodes, you must first install the Unified Communications Manager locale file for the same country on the Unified Communications Manager cluster.
Procedure

**Step 1** Find the locale installer for your release on cisco.com:

- For Cisco Unified Communications Manager, go to [https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm](https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm)

**Step 2** Download your release's locale installer to a server that supports SFTP. You need the following files:

- User Locale files—These files contain language information for a specific language and country and use the following convention:
  - cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
  - ps-locale-language_country-version.cop (IM and Presence Service)

- Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:
  - cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

**Step 3** Log in to Cisco Unified OS Administration using the administrator account.

**Step 4** Choose Software Upgrades > Install/Upgrade.

**Step 5** Complete the following fields in the Software Installation/Upgrade window:

- For the Source, choose Remote file System.
- From the Directory, enter the path to the directory where you saved the locale installer.
- From the Server field, enter the server name for the remote file system.
- Enter the credentials for the remote file system.
- From the Transfer Protocol drop-down list, choose SFTP. You must use SFTP for the transfer protocol.

**Step 6** Click Next.

**Step 7** Download and install the locale on the server.

**Step 8** Restart the server. The updates take effect after the server restarts

**Step 9** Repeat this procedure on all Unified Communications Manager and Instant Messaging and Presence cluster nodes in the prescribed order.
Do not reset user locales for your end users until the new locale is installed on all cluster nodes. If you are installing the locale for both Unified Communications Manager and Instant Messaging and Presence Service, you must install the locale for both products before you reset user locales. If you run into any issues, such as could occur if an end user resets a phone language before the locale installation is complete for Instant Messaging and Presence Service, have your users reset their phone language in the Self-Care Portal to English. After the locale installation is complete, users can reset their phone language, or you use Bulk Administration to synchronize locales to the appropriate language by bulk.

---

**Note**

---

**Restore the Database Replication Timeout**

This procedure applies to Unified Communications Manager nodes only.

Use this procedure if you increased the database replication timeout value before you began the upgrade process.

The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the Unified Communications Manager subscriber nodes have successfully set up replication.

**Procedure**

**Step 1**

Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh adminname@hostname` and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

**Step 2**

Execute the `utils dbreplication setrepltimeout timeout` command, where `timeout` is database replication timeout, in seconds. Set the value to 300 (5 minutes).

---

**Verify the Registered Device Count**

Use the Real Time Monitoring Tool (RTMT) to view the device count and verify your endpoints and resources after the upgrade is complete.

**Procedure**

**Step 1**

From the Unified RTMT interface, select Voice/Video > Device Summary.

**Step 2**

Record the number of registered devices:

<table>
<thead>
<tr>
<th>Item</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Phones</td>
<td></td>
</tr>
<tr>
<td>Registered Gateways</td>
<td></td>
</tr>
</tbody>
</table>
Verify Assigned Users

Use this procedure to verify the number of assigned users on nodes after the upgrade is complete.

Procedure

Step 1
From the Cisco Unified CM IM and Presence Administration interface, select **System > Cluster Topology**.

Step 2
Compare this information to the number of assigned users that you recorded before the upgrade and ensure that there are no errors.

Test Functionality

After the upgrade, perform the following tasks:

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line

- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
• Do Not Disturb
• Privacy
• Presence
• CTI call control
• Busy Lamp Field

• Test Instant Messaging and Presence functions:
  • Basic presence states, such as available, unavailable, and busy
  • Send and receive files
  • Advanced features, such as persistent chat, federated users, and message archiving

Upgrade RTMT

Tip
To ensure compatibility, Cisco recommends that you upgrade RTMT after you complete the Unified Communications Manager upgrade on all servers in the cluster.

RTMT saves user preferences and downloaded module jar files locally on the client machine. The system saves user-created profiles in the database, so you can access these items in Unified RTMT after you upgrade the tool.

Before you begin
Before you upgrade to a newer version of RTMT, Cisco recommends that you uninstall the previous version.

Procedure

Step 1
From Unified Communications Manager Administration, choose Application > Plugins.

Step 2
Click Find.

Step 3
Perform one of the following actions:
  • To install the tool on a computer that is running the Microsoft Windows operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Windows.
  • To install the tool on a computer that is running the Linux operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Linux.

Step 4
Download the installation file to your preferred location.

Step 5
Locate and run the installation file.
The extraction process begins.

Step 6
In the RTMT welcome window, click Next.

Step 7
Because you cannot change the installation location for upgrades, click Next.
The Setup Status window appears; do not click Cancel.
Step 8  
In the Maintenance Complete window, click Finish.

---

Manage TFTP Server Files

You can upload files for use by the phones to the TFTP server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the `tftp` directory by default. You can also upload files to a subdirectory of the `tftp` directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all nodes, nor to both Cisco TFTP servers in a cluster.

To upload and delete TFTP server files, follow this procedure:

**Procedure**

**Step 1**

From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades > TFTP > File Management**.

The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

**Step 2**

To upload a file, follow this procedure:

a) Click **Upload File**.

   The Upload File dialog box opens.

b) To upload a file, click **Browse** and then choose the file that you want to upload.

c) To upload the file to a subdirectory of the `tftp` directory, enter the subdirectory in the **Directory** field.

d) To start the upload, click **Upload File**.

   The Status area indicates when the file uploads successfully.

e) After the file uploads, restart the Cisco TFTP service.

   **Note**  
   If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.

   For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide*.

**Step 3**

To delete files, follow this procedure:

a) Check the check boxes next to the files that you want to delete.

   You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

b) Click **Delete Selected**.
If you want to modify a file that is already in the tftp directory, you can use the CLI command `file list tftp` to see the files in the TFTP directory and `file get tftp` to get a copy of a file in the TFTP directory. For more information, see Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

---

**Set Up a Custom Log-On Message**

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface.

To upload a customized log-on message, follow this procedure:

**Procedure**

**Step 1**
From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades > Customized Logon Message**.

The Customized Logon Message window displays.

**Step 2**
To choose the text file that you want to upload, click **Browse**.

**Step 3**
Click **Upload File**.

**Note** You cannot upload a file that is larger than 10kB.

The system displays the customized log-on message.

**Step 4**
To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

**Note** Check the **Require User Acknowledgment** checkbox if you want the custom message to be displayed on the login screens of the Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface.

---

**Configure IPSec Policies**

Use this procedure only if you are performing a PCD migration from Release 6.1(5). You must recreate your IPSec policies after the PCD migration is complete, because IPSec policies from Release 6.1(5) are not migrated to the new release.

- IPsec requires bidirectional provisioning, or one peer for each host (or gateway).
• When you provision the IPSec policy on two Unified Communications Manager nodes with one IPSec policy protocol set to “ANY” and the other IPSec policy protocol set to “UDP” or “TCP”, the validation can result in a false negative if run from the node that uses the “ANY” protocol.

• IPSec, especially with encryption, affects the performance of your system.

Procedure

Step 1 From Cisco Unified OS Administration, choose Security > IPSec Configuration.
Step 2 Click Add New.
Step 3 Configure the fields on the IPSec Policy Configuration window. See the online help for more information about the fields and their configuration options.
Step 4 Click Save.
Step 5 (Optional) To validate IPSec, choose Services > Ping, check the Validate IPSec check box, and then click Ping.

Assign New Manager Assistant Roles

Perform this procedure only if your previous release was configured to use the Cisco Unified Communications Manager Assistant feature, and you assigned application users to use either the InterCluster Peer-User or the Admin-CUMA roles. The InterCluster Peer-User and Admin-CUMA roles are deprecated from release 10.0(1) onward and are removed during the upgrade process. You must assign new roles for those users.

Procedure

Step 1 To configure roles and users, see the chapter Manage Users in Administration Guide for Cisco Unified Communications Manager.
Step 2 Ensure that the AXL user defined on the Instant Messaging and Presence service user interface (Presence > Inter-Clustering) has a Standard AXL API Access role associated with it on the Unified Communications Manager application user page.

Verify IM and Presence Service Data Migration

When you upgrade from Cisco Unified Presence Release 8.x to an Instant Messaging and Presence Service release, user profiles are migrated to Unified Communications Manager. The user profile information is stored as new service profiles on Unified Communications Manager with the following name and description format:

Name: UCServiceProfile_Migration_x (where x is a number starting at 1)
Description: Migrated Service Profile Number x

To ensure that users can successfully log into Cisco Jabber after an upgrade from Cisco Unified Presence Release 8.x, you must verify that the user profile data migration was successful.

Profiles that are created but that are not assigned to users are not migrated to Unified Communications Manager.
**Procedure**

**Step 1** From Cisco Unified CM Administration, select User Management > User Settings > Service Profile.

**Step 2** Select Find to list all service profiles.

**Step 3** Verify that there are migrated service profiles with the following name format:  *UCServiceProfile_Migration_x*.

**Step 4** If there are no migrated service profiles, check the *installdb log* file for any errors.

**Step 5** If the data migration fails, an import error alarm is raised on Unified Communications Manager and the Cisco Sync Agent sends a failure notification to the Cisco Unified CM IM and Presence Administration GUI.

**Tip** To view the alarm details, log into RTMT for Cisco Unified Communications Manager.

**What to do next**

You can edit these service profiles to give them more meaningful names. See Administration Guide for Cisco Unified Communications Manager for more information about configuring service profiles.

### Enable High Availability on Presence Redundancy Groups

This procedure applies to Instant Messaging and Presence nodes only. If you disabled high availability on presence redundancy groups before beginning the upgrade process, use this procedure to enable it now.

**Before you begin**

If it has been less than 30 minutes since your services restarted, confirm that your Cisco Jabber sessions have been recreated before you enable High Availability. Otherwise, Presence will not work for Jabber clients whose sessions aren't created.

To obtain the number of Jabber sessions, run the *show perf query counter "Cisco Presence Engine" ActiveJamSessions* CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability prior to the upgrade.

**Procedure**

**Step 1** From the Cisco Unified CM Administration user interface, choose System > Presence Redundancy Groups.

**Step 2** Click Find and select the Presence Redundancy Group. The Presence Redundancy Group Configuration window displays.

**Step 3** Check the Enable High Availability check box.

**Step 4** Click Save.

**Step 5** Repeat this procedure in each Presence Redundancy Group.
Restart the IM and Presence Sync Agent

If you stopped the Instant Messaging and Presence Sync Agent service before you began the upgrade process, restart it now.

Procedure

Step 1  From the Cisco Unified Serviceability interface, select **Tools > Control Center - Network Services**.

Step 2  Select an Instant Messaging and Presence node from the **Server** drop-down list and click **Go**.

Step 3  In the **IM and Presence Services** section, select the **Cisco Sync Agent** and click **Restart**.

Example

Note  After the Cisco Intercluster Sync Agent has finished the initial synchronisation, manually load the new Tomcat certificate onto Unified Communications Manager. This ensures that the synchronisation does not fail.