Upgrade Tasks

Upgrade Overview

Use the procedures in this chapter to complete one of the following upgrade types using either the Cisco Unified OS Admin GUI or the CLI. For procedures, refer to the task flow that covers your upgrade type.

- Clusterwide Upgrades (Direct Standard)—Pre-upgrade version must be 12.5(1) minimum. Otherwise, you must use the other method.
- Upgrade Cluster Nodes (Direct Standard)

Note Direct upgrades from pre-12.5 source to Release 15 is not supported.

Note If your Unified Communications Manager publisher node is on Release 15 and the subscribers nodes are in Release 12.5.x or 14 and SUs, the nodes in the cluster will not be authenticated. Only when the subscribers nodes are upgraded to Release 15, all the nodes will be in the authenticated state.

Note For upgrades and migrations that use Cisco Prime Collaboration Deployment, see the Cisco Prime Collaboration Deployment Administration Guide to set up an upgrade task or migration task.

Before You Begin

Caution Stop all configuration tasks. Don't make any configuration changes during the upgrade. For example, don't change passwords, perform LDAP synchronizations, or run any automated jobs. Don't remove, readd, or reinstall any nodes in the cluster during the upgrade process. You can make configuration changes only when you have completed the upgrade on all nodes and completed postupgrade tasks. The upgrade overwrites configuration changes that you make during the upgrade, and some configuration changes can cause the upgrade to fail.

We recommend that you suspend user synchronization with LDAP. Don't resume synchronization until you have completed the upgrade on all Unified Communications Manager and IM and Presence Service cluster nodes.

- Don't rename or compress the upgrade file. Otherwise, the system rejects the file as a valid upgrade file.
- For IM and Presence Service upgrades, check that the contact list size for users is below the maximum. Use the System Troubleshooter in Cisco Unified CM IM and Presence Administration to verify that no users have exceeded the limit.
- Modify the network adapter to VMXNET3 before the upgrade process. For details, see your OVA readme file.
- If you're upgrading a node in FIPS mode, make sure that your security password has a minimum of 14 characters. To change passwords, see the 'Reset the Administrator or Security Password' section in the "Getting Started" chapter of the Administration Guide for Cisco Unified Communications Manager.

Note From Release 12.5(1) SU2 onwards, it's recommended to perform both the upgrade stages [Install and Switch Version] during the same Maintenance Window to avoid an impact on the other AXL-dependent integrations.

Note During the switch version, only User Facing Features (UFF) in dynamic tables (numplandynamic, devicedynamic, and more) gets updated. Other tables are migrated during the upgrade. Any configuration changes after the upgrade or before the switch versions are lost.

Note In the upgrade logs, it's observed that there is time discrepancy or time jumps during certain intervals. This time jump is an expected behavior since the hardware clock is disabled until the system synchronizes with the NTP server.

Note If you have different security passwords in the active and inactive versions, and when you switch back to a lower version, ensure that you change the security password in the lower version to be same as the higher version. Follow these steps to change the security password:

1. Switch the publisher node to a lower version.
2. Change the security password of the publisher node to the new password which is same as the higher version.
3. Switch the subscriber to a lower version.
4. Change the security password of the subscriber node to the new password which is same as the higher version.

Note Use this procedure to verify the NTP configurations before you upgrade to Release 15:

1. Ensure that you always use an NTP source with lesser offset and jitter from a reliable source.
2. We recommend that you have one good NTP server configured for time synchronization. If you are configuring more than one NTP server, you must configure a minimum of four NTP servers so that chrony can have a tie breaker if each of the clocks is pointing to different time zones.
3. You must always upgrade ESXi to match the compatible versions supported by the Cisco Voice Operating System (VOS) servers.
4. During network migrations between different hosts, ensure that you use the same NTP source (OR) NTP source with a reliable clock.

Download Upgrade Files

Before you upgrade, download the files that you need:.

Note To optimize the upgrade, make sure to save the downloaded files in the same directory.

Table 1: Upgrade Files to Download

Files to Download	Download Site
Unified CM Upgrade ISO	Go to Unified Communications Manager Downloads—Select your version and then look under **Unified Communications Manager Updates** for upgrade ISOs. For example, `UCSInstall_UCOS_<XXXXXXXX>.sha512.iso`.
IM and Presence Service Upgrade ISO	Go to IM and Presence Service Downloads—Select your version and look under **Unified Presence Server (CUP) updates** for upgrade ISOs. For example, `UCSInstall_CUP_<XXXXXXXX>.sha512.iso`.

Files to Download	Download Site
Upgrade Readiness COP Files (pre-upgrade and post-upgrade)	You can download the pre-upgrade COP file and post-upgrade COP file from either of the above download sites: • For Unified CM, the COP files appear under **Unified Communications Manager Updates** • For IM and Presence Servivce, the COP files appear under **Unified Presence Server (CUP) Updates > UTILS** For example, `ciscocm.preUpgradeCheck-XXXXX.cop.sgn` and `ciscocm.postUpgradeCheck-XXXXX.cop.sgn` **Note** When you try to upgrade, using COP files it shows the number of files installed in the system. Once the upgrade is done the list of COP files will not match previous versions. If you need the previous files you need to install COP files manually.

Clusterwide Upgrade Task Flow (Direct Standard)

Complete the following tasks to complete a simplified clusterwide upgrade. This will complete a clusterwide direct standard upgrade.

Note The Clusterwide Upgrade option is available only for direct standard upgrades where the pre-upgrade version is a minimum release of 12.5(1).

Note Ensure that you verify the software location details of each node before you start the upgrade process.

Before you begin

Download upgrade ISO files and Upgrade Readiness COP files and save them in the same directory. For download information, go to Download Upgrade Files, on page 3.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 5	Run the Upgrade Readiness COP file to check connectivity and health of the system. If there are issues, fix them before proceeding with the upgrade.
Step 2	Configure Clusterwide Reboot Sequence, on page 7	Specify the reboot sequence beforehand in order to minimize downtime.

	Command or Action	Purpose
Step 3	Configure Cluster Software Location, on page 7	Before upgrade, you can choose to configure the cluster software location details for all the nodes associated within the cluster.
Step 4	Upgrade the cluster using either one of these methods: • Complete Clusterwide Upgrade via OS Admin, on page 8 • Complete Clusterwide Upgrade via CLI, on page 9	During the upgrade, you can switch versions automatically as a part of the upgrade, or you can save the upgraded version to the inactive partition.
Step 5	Switch Version Manually (Clusterwide), on page 10	Optional. If you chose not to switch versions automatically during the upgrade, switch versions manually.
Step 6	Run Upgrade Readiness COP File (Post-upgrade), on page 11	Run the post-upgrade COP file to guage the post-upgrade health of your system.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count

- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Run the COP file again.
d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double-click on nodes, expand **CUCM Publisher > System > Install upgrade Logs**.
f) Double-click on **Install** and select the file which you require and download.

Configure Clusterwide Reboot Sequence

For simplified cluster-wide upgrades, use this procedure before you upgrade to set the reboot sequence for the cluster upgrade. This option is available only if the pre-upgrade version is 12.5(1) minimum.

Note If you don't configure a reboot sequence, the clusterwide upgrade uses the last saved reboot sequence or the default sequence.

Procedure

Step 1 On the publisher node, login to Cisco Unified OS Administration or Cisco Unified CM IM and Presence OS Administration.

Step 2 Choose **Software Upgrades** > **Restart/Switch-Version Cluster**.
The **Reboot Cluster Settings** window appears with sliders that display the reboot sequence per node.

Step 3 Use the sliders to adjust the reboot sequence according to your needs.

Step 4 Click **Save**.

What to do next

Complete one of the following tasks, depending on which interface you want to use:

- Complete Clusterwide Upgrade via OS Admin, on page 8
- Complete Clusterwide Upgrade via CLI, on page 9

Configure Cluster Software Location

Use this procedure to add, edit, or modify any of the existing configurations for a node in the same cluster.

Note You may only use this feature if all the nodes in your cluster are Release 14SU2 or later.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** user interface.

Step 2 Choose **Software Upgrades > Cluster Software Location**.

Step 3 Select a node to add or edit the server location details from the list.

Step 4 Check the **Apply to All Nodes** check box if you want the same software location details to be applied for all the other nodes in the cluster including the publisher.

This check box is displayed only when you select the Unified CM publisher from the **Select Node** drop-down list.

Step 5 Use the **Use download credentials and software location from Publisher** if you want to use the source configuration and software location details from the publisher node.

By default, the **Use download credentials and software location from Publisher** option is selected.

Note This option is available only for the subscriber nodes.

Step 6 (Optional) If you do not want to use the **Use download credentials and software location from Publisher** option, use the **Use below download credentials and software location** option before you upgrade your server.

Note This option is available only for the subscriber nodes.

Step 7 From the **Source** drop-down list, select the option that matches where the upgrade file is saved:

- **DVD/CD**
- **Local filesystem**—This option is available only if you are resuming a previous upgrade that was cancelled
- **SFTP server**—You must also enter the SFTP server details, including the Directory, Server address and login credentials.

Step 8 (Optional) To receive an email notification when the upgrade is complete, enter the **SMTP Server** address and an **Email Destination** so that you can be emailed when the upgrade completes.

Step 9 Check the **Continue with upgrade after download** check box if you want the upgrade to commence automatically once the upgrade file is downloaded. If you don't check this check box, you will need to manually initiate the upgrade later using **Local filesystem** as the **Source**.

Step 10 Check the **Switch-version server after upgrade (valid only for ISO)** check box to reboot the system automatically after the completion of successful upgrade.

Step 11 Click **Save** to update all the configuration changes for that particular node that is added or modified.

Complete Clusterwide Upgrade via OS Admin

Use this procedure to complete a simplified clusterwide upgrade of Unified Communications Manager and the IM and Presence Service. This option is available for standard upgrades only where the pre-upgrade version is 12.5(1) or later.

Note You can also complete a standard clusterwide upgrade by running the `utils system upgrade cluster` CLI command.

Before you begin

Make sure that you have downloaded the upgrade file to a location that you can access.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** or **Cisco Unified IM and Presence OS Administration**.

Step 2 Choose **Software Upgrades > Install/Upgrade Cluster**. This option is not available if the From version is pre-12.5(1).

Step 3 You can view the following configuration information required to upgrade an existing node:

Note In Release 14 SU2 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface.

- **Credentials Information—**Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**— Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 Click **Next**.

Step 5 Select the upgrade version that you want to install, and click **Next**.
The upgrade commences. The **Installation Status** page displays information about the upgrade.

Note During cluster wide upgrade, make sure to have the first 3 digits common between the selected Unified Communications Manager and IM and Presence Service upgrade files.

Step 6 Click **Finish** when the upgrade completes.
If you chose to switch versions automatically, the cluster reboots to the upgraded version according to the cluster reboot sequence. Otherwise, the upgrade saves to the inactive partition and you must switch versions manually in order to use the upgraded software.

Complete Clusterwide Upgrade via CLI

Use this procedure to complete a simplified clusterwide upgrade using the Command Line Interface.

Note This option is available only for direct standard upgrades where the pre-upgrade version is Release 12.5(x) or later.

Before you begin

Configure Clusterwide Reboot Sequence, on page 7—If you want to switch versions automatically after the upgrade, set the reboot sequence beforehand. Otherwise, the cluster reboots using the last saved sequence. If no reboot sequence has been saved, the default sequence is used.

Note In Release 14 SU2 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

Procedure

Step 1 Log in to the Command Line Interface on the Unified CM publisher node.

Step 2 Run the `utils system upgrade cluster` CLI command and the wizard displays the software location details to configure all the nodes in the same cluster.

Step 3 You can view the following configuration information required to upgrade an existing node:

- **Credentials Information—**Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**— Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 If you are prompted to start the installation, enter **Yes**.
If you chose to switch versions automatically after the upgrade, the cluster reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Switch Version Manually (Clusterwide)

Use this procedure for Direct Standard Upgrades where you switch the inactive and active versions across all cluster nodes through the Unified Communications Manager publisher node without having to UI or CLI to any other nodes.

Note You can use this procedure only for:

- Direct Standard Upgrades
- Using Simple Upgrades cluster-wide automation
- Pre-upgrade version 12.5(1) or later

Note The Add/update/delete functionalities will not be allowed as one or more cluster nodes are not yet finished with one or more of upgrading the inactive versions, switch-version reboots and database replication. From the Cisco Unified OS Administration UI, navigate to **Software Upgrade > Install/Upgrade** or **Software Upgrade > Cluster Install/Upgrade** to view the upgrade status. Or, execute the commands **utils system upgrade status** or **utils system cluster upgrade status** to monitor the upgrade status. See Upgrade and Migration Overview for more information.

Procedure

Step 1 Log in to Cisco Unified OS Administration or Cisco Unified CM IM and Presence OS Administration.

Step 2 Choose **Software Upgrades** > **Reboot Cluster**.

Step 3 Optional. If you haven't already configured the reboot sequence, use the sliders to edit the reboot sequence and click **Save**.

Step 4 Click **Switch Versions**.

Note If you prefer to use CLI, note that there is no CLI for Simple Upgrades cluster switch version automation. You can instead use the single-node switch version with the `utils system switch-version` CLI command, but this must be done on a node-by-node basis.

Run Upgrade Readiness COP File (Post-upgrade)

After upgrading, run the post-upgrade COP file, which checks the following:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- FIPS mode password length restrictions
- Licensing sync
- VMware tools compatibility
- Disk space

- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameter settings
- TFTP Maximum Service Counts
- Active and Inactive versions

Note It's strongly recommended that you run the Upgrade Readiness COP file for post-upgrade checks after you upgrade in order to verify the health of your system.

Procedure

Step 1 Download the Upgrade Readiness COP file to run post upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.postUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version.).

Step 2 Check your post-upgrade system health:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Repeat these steps until the COP file returns no errors.

Step 3 To view the reports from CLI for post-upgrade run **file get install/PostUpgradeReport.txt** command.

Step 4 To view the report from RTMT

a) Login into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double click on nodes, expand **CUCM Publisher > System > Install upgrade Logs**.
f) Double click on **Install** and select the file which you require and download.

What to do next

The upgrade is complete. You can begin using the new software.

Upgrade Cluster Nodes (Direct Standard)

Complete these tasks to upgrade cluster nodes on a node by node basis. You must use this process if you are completing a direct standard upgrade using the Unified OS Admin or CLI interfaces.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Before you begin

Download upgrade ISO files and Upgrade Readiness COP files and save them in the same directory. For download information, go to Download Upgrade Files, on page 3.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 5	Run the Upgrade Readiness COP file to check connectivity and health of the system. If there are issues, fix them before proceeding with the upgrade.
Step 2	Configure Cluster Software Location, on page 7	Before upgrade, you can choose to configure the cluster software location details for all the nodes associated within the cluster.
Step 3	Upgrade cluster nodes using either the GUI or CLI interfaces. • Upgrade Cluster Nodes via OS Admin (Direct Standard), on page 16 • Upgrade Cluster Nodes via CLI (Direct Standard), on page 17	Upgrade the cluster nodes in your cluster.
Step 4	Switch Versions Manually, on page 19	Optional. If you did not switch versions automatically during the upgrade, use this procedure to switch versions manually.
Step 5	Run Upgrade Readiness COP File (Post-upgrade), on page 19	After the upgrade, run the post-upgrade COP file to gauge the post-upgrade health of your system.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Run the COP file again.
d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double-click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double-click on **Install** and select the file which you require and download.

Configure Cluster Software Location

Use this procedure to add, edit, or modify any of the existing configurations for a node in the same cluster.

Note You may only use this feature if all the nodes in your cluster are Release 14SU2 or later.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** user interface.

Step 2 Choose **Software Upgrades** > **Cluster Software Location**.

Step 3 Select a node to add or edit the server location details from the list.

Step 4 Check the **Apply to All Nodes** check box if you want the same software location details to be applied for all the other nodes in the cluster including the publisher.

This check box is displayed only when you select the Unified CM publisher from the **Select Node** drop-down list.

Step 5 Use the **Use download credentials and software location from Publisher** if you want to use the source configuration and software location details from the publisher node.

By default, the **Use download credentials and software location from Publisher** option is selected.

Note This option is available only for the subscriber nodes.

Step 6 (Optional) If you do not want to use the **Use download credentials and software location from Publisher** option, use the **Use below download credentials and software location** option before you upgrade your server.

Note This option is available only for the subscriber nodes.

Step 7 From the **Source** drop-down list, select the option that matches where the upgrade file is saved:

- **DVD/CD**
- **Local filesystem**—This option is available only if you are resuming a previous upgrade that was cancelled
- **SFTP server**—You must also enter the SFTP server details, including the Directory, Server address and login credentials.

Step 8 (Optional) To receive an email notification when the upgrade is complete, enter the **SMTP Server** address and an **Email Destination** so that you can be emailed when the upgrade completes.

Step 9 Check the **Continue with upgrade after download** check box if you want the upgrade to commence automatically once the upgrade file is downloaded. If you don't check this check box, you will need to manually initiate the upgrade later using **Local filesystem** as the **Source**.

Step 10 Check the **Switch-version server after upgrade (valid only for ISO)** check box to reboot the system automatically after the completion of successful upgrade.

Step 11 Click **Save** to update all the configuration changes for that particular node that is added or modified.

Upgrade Cluster Nodes via OS Admin (Direct Standard)

Use this procedure to complete a direct standard upgrade of Cisco Unified Communications Manager or IM and Presence Service cluster nodes.

Note Some upgrade options may differ slightly depending on which version you are upgrading from.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** or **Cisco Unified IM and Presence OS Administration**.

Step 2 Choose **Software Upgrades > Install/Upgrade**.

Step 3 You can view the following configuration information required to upgrade an existing node:

Note In Release 14SU3 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

- **Credentials Information**—Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**—Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 Click **Next**.

Step 5 Select the upgrade version that you want to install, and click **Next**.
The upgrade commences. The **Installation Status** page displays information about the upgrade.

Step 6 Click **Finish** when the upgrade completes.
If you chose to switch versions automatically after the upgrade, the node reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Step 7 Repeat this procedure for additional cluster nodes.

Upgrade Cluster Nodes via CLI (Direct Standard)

Use this procedure to upgrade individual cluster nodes via the CLI.

Note Upgrade options may differ depending on which version you are upgrading from.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Note In Release 14SU3 onwards, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

Procedure

Step 1 Log in to the Command Line Interface on the node that you want to upgrade.

Step 2 Run the `utils system upgrade initiate` CLI command and the wizard displays the software location details to configure all the nodes in the same cluster.

Step 3 When prompted, choose one of the following:

- If you choose **Yes**, the upgrade process checks for the upgrade files that you can use as the source file and proceeds to step **8**.
- If you choose **No**, you are prompted to choose the source (follow steps **4** to **8**).

Step 4 When prompted, choose the source where the upgrade file is saved:

- **Remote filesystem via SFTP or FTP**—You will be prompted to enter the server details and credentials.
- **Local DVD/CD**—The local CD or DVD only.
- **Local image**—This option is available only if you initiated an upgrade earlier and did not complete the upgrade.

Step 5 (Optional) Enter an **SMTP Host** for email notifications that tell you when the upgrade is complete.

Step 6 When prompted, enter whether to proceed with the upgrade automatically after the upgrade file downloads.

- **Yes**—The upgrade commences once the file downloads to all nodes.
- **No**—The upgrade file gets saved as a Local Image. You can restart the upgrade later.

Step 7 When prompted, enter whether to switch versions automatically after the upgrade:

- **Yes**—After the upgrade, the cluster switches to the new version and reboots automatically.
- **No**—The upgrade saves to the Inactive Partition. You can switch versions manually later.

Step 8 When prompted to start the installation, enter **Yes**.
If you chose to switch versions automatically after the upgrade, the node reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Switch Versions Manually

If you did not switch versions automatically as a part of the upgrade, you can use this procedure to switch versions for cluster nodes manually. You can use either the GUI or the CLI.

Note The clusterwide version switch option is available only for direct standard upgrades where the pre-upgrade version is a minimum release of 12.5(x). For details, Switch Version Manually (Clusterwide), on page 10

Procedure

Step 1 If you want to use the GUI:

a) Log in to the Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration interface for the node that you want to switch and do the following:
b) Choose **Settings** > **Version**.
c) Verify the version of the active and inactive software.
d) Click **Switch Version**s to switch versions and restart the node.
e) Repeat these steps for additional cluster nodes.

Step 2 If you want to use the CLI:

a) Log in to the Command Line Interface for the node.
b) Run the `utils system switch-version` CLI command.
c) Repeat these steps for additional cluster nodes.

Run Upgrade Readiness COP File (Post-upgrade)

After upgrading, run the post-upgrade COP file, which checks the following:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- FIPS mode password length restrictions
- Licensing sync
- VMware tools compatibility
- Disk space
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Services status

- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameter settings
- TFTP Maximum Service Counts
- Active and Inactive versions

Note It's strongly recommended that you run the Upgrade Readiness COP file for post-upgrade checks after you upgrade in order to verify the health of your system.

Procedure

Step 1 Download the Upgrade Readiness COP file to run post upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.postUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version.).

Step 2 Check your post-upgrade system health:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Repeat these steps until the COP file returns no errors.

Step 3 To view the reports from CLI for post-upgrade run **file get install/PostUpgradeReport.txt** command.

Step 4 To view the report from RTMT

a) Login into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double click on nodes, expand **CUCM Publisher > System > Install upgrade Logs**.
f) Double click on **Install** and select the file which you require and download.

What to do next

The upgrade is complete. You can begin using the new software.

Switch Cluster to Previous Version

To switch a cluster back to a previous version, complete these high-level tasks:

Procedure

Step 1 Switch back the publisher node.

Step 2 Switch back all backup subscriber nodes.

Step 3 Switch back all primary subscriber nodes.

Step 4 If you are reverting to an older product release, reset database replication within the cluster.

Switch Node to Previous Version

Procedure

Step 1 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence Service 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 2 Choose **Settings** > **Version**.

The Version Settings window displays.

Step 3 Click the **Switch Versions** button.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4 To verify that the version switch was successful, follow these steps:

a) Log in again to the management software for the node that you are upgrading.

b) Choose **Settings** > **Version**.

The Version Settings window displays.

c) Verify that the correct product version is now running on the active partition.

d) Verify that all activated services are running.

e) For the publisher node, log in to Cisco Unified CM Administration.

f) Verify that you can log in and that your configuration data exists.

Reset Database Replication

If you switch back the servers in a cluster to run an older product release, you must manually reset database replication within the cluster.

Procedure

Step 1 Log in to the Command Line Interface on the publisher node.

Step 2 Run the `utils dbreplication reset all` command.