Upgrading Cisco Unity Connection

Introduction

You need to upgrade from the current version of Cisco Unity Connection to a higher version to use the new features supported with the new version. When you upgrade a server, the new version of Unity Connection is installed in a separate disk partition known as inactive partition. To activate the new version, you need to perform switch version. The following are the two ways to switch to the new version:

- Automatic Switching: Allows you to automatically switch to the new version of Unity Connection as part of the upgrade process.
- Manual Switching: Allows you to manually switch to the new version of Unity Connection after the successful completion of upgrade.

If you need to revert the server to the previous version, you can rollback to the previous version.

Upgrade Types

The Unity Connection upgrade files are available as ISO images or COP (Cisco Option Package) files. You can use either of the following interfaces to upgrade Unity Connection:

- Command Line Interface (CLI)
- Cisco Unified OS Administration web interface.

You must save the COP files on a Network Location FTP/SFTP server accessible during upgrade. ISO image can be saved on a local DVD or on a network location. The performance of the upgrades can be monitored through CLI or Cisco Unified Operating System Administration interfaces.

Table 1: Upgrade Matrix for Cisco Unity Connection explains the upgrade types and supported upgrade paths from one version to another.

Table 1: Upgrade Matrix for Cisco Unity Connection

Upgrade Type	Upgrade Path	Description
Refresh Upgrade (RU)	• For 11.5 to 15, you must follow an intermediate upgrade path. Example: 11.5 to 12.5 or later and then 12.5 or later to 15.	• If the operating system version of the Unity Connect during an upgrade, it is referred to as a Refresh Upg **Note** • You need the following COP file before 11.5 or later to 15 : ciscocm.CSCwi52160_15-direct-migration_ . • Refresh Upgrades from Pre-12.5.x sour not supported. • A fresh installation with data import is a direct upgrades from releases 11.5 and a For more information, see Install with D
Level 2 (L2)	12.5.1SU3 or earlier to 15	• If the operating system version of the Unity Connect change during an upgrade, it is referred to as an Lev upgrade. • You need the following COP file before performing t • ciscocm.CSCwi52160_15-direct-migration_v1.0.k • ciscocm.enable-sha512sum-2021-signing-key-v • The new version is installed on the inactive partition t can switch later on.
	• 12.5.1SU4 or later to 15 • 14 or later to 15	• You need the following COP file before performing t ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.
COP file, for more information, see the Applying COP file from a Network Location	Fix for the same version	• COP files are installed on the active partition and yo uninstall them. Contact Cisco TAC to uninstall COP

Note If you are upgrading Unity Connection to 15 and later, then after completion of successful upgrade, you must reinstall the set of available locales that are compatible with the upgraded version.

Before installing locales, you must stop the Connection Conversation Manager and Connection Mixer services through Cisco Unity Connection Serviceablity page. Otherwise, you may not get the proper installation status on GUI. It is recommended that you should install the locales on Unity Connection through Command Line Interface.

For more information on CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Caution After successful upgrade to Unity Connection 15, if you need to revert the server to previous software version, you can switch version the software to older version. After that, you can not upgrade the server to any pre 15 release (for example: 11.5(1) or 12.0(1)). In addition to this, if the upgrade from any previous releases to Unity Connection 15 fails for any reason, then also you cannot upgrade the server to pre 15 release. To troubleshoot the issue, contact Cisco TAC.

If administrator wants to upgrade the server to pre 15 release in above scenarios, fresh cluster rebuild is required by performing DRS backup and restore before upgrade.

If you are upgrading Unity Connection from 11.5(1) or 12.0(1) as base release to 15 and later, then you must rename custom role "Read Only Administrator" to different name on base release before upgrade.

Note The procedure for upgrading Unity Connection to any Service Update (SU), is similar to RU and L2 upgrade.

Status of Unity Connection Cluster During an Upgrade

When a Unity Connection cluster is upgraded, the publisher server is completely disabled for the entire duration of upgrade but the subscriber server continues to provide services to users and callers. However, the performance of the cluster is affected in the following ways:

- If the phone system is routing calls to the subscriber server, outside callers and Unity Connection users can leave voice messages but the messages are not immediately delivered to user mailboxes. During switch version on the subscriber server in a cluster, messages that were left on the subscriber server are copied to the publisher server and delivered to user mailboxes.
- Unity Connection users can use the telephone user interface (TUI) to play messages recorded before the upgrade starts but cannot play the messages recorded during the upgrade.
- Unity Connection may not retain the status of messages. For example, if a user plays a message during the upgrade, the message may be marked as new again after the upgrade. Likewise, if a user deletes a message during the upgrade, the message may reappear after the upgrade.

- User can access Unity Connection using clients such as, ViewMail for Outlook, Web Inbox and Jabber during upgrade. However, during switch version, user cannot access these clients. In case of RU, these clients are not accessible during complete upgrade..
- Administrator users can make configuration changes using any of the administration applications, such as Cisco Unity Connection Administration and Cisco Unified Operating System Administration during upgrade. However, Unity Connection does not allow provisioning and configuration changes through administration applications or VMREST during the switch version. In case of RU, provisioning and configuration are not allowed in complete upgrade duration.
- Intrasite, intersite or HTTPS networking with other servers is disabled for the duration of the switch version. Directory changes made on the other servers in the network are not replicated to the server or cluster until the switch version is complete.

Duration of Upgrade

Under ideal network conditions, an upgrade process takes approximately two hours to complete on each server. Therefore, a Unity Connection cluster takes four hours to upgrade to a higher version. Depending on the data size of the server, the switch version process might take some more time.

If you are upgrading in a slow network condition, the upgrade process may take longer time than expected. It is always recommended to upgrade Unity Connection during off-peak hours or during a maintenance window to avoid service interruptions.

Tip You can reduce the duration of upgrade process by asking users to permanently delete items in the deleted items folder before starting the upgrade. This saves time as deleted items are not copied.

Prerequisites for Upgrade

Before beginning the upgrade process, you must consider the following points for a successful upgrade:

- Ensure that you have a good network connection to avoid service interruptions during upgrade.
- You must have a Secure File Transfer Protocol (SFTP) or File Transfer Protocol (FTP) server in place when upgrading from a network location.
- Check the current version and determine the version to which you want to upgrade. See the release notes of the new version for more information. Release notes are available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.
- Determine if you need COP files depending on the upgrade process. Download the COP and ISO image files from: http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm
- Backup all the existing data. For more information on backup and restore, see the Introduction chapter.
- Update the following virtual machine settings on both publisher and subscriber server through VMware vSphere client.

Note For more information on changing the Guest Operating System and network adapter, see the corresponding Readme of the OVA template at https://software.cisco.com/download/home/283062758/type.

- Confirm that the status of both publisher and subscriber servers is active and they can answer calls. Follow the given steps to confirm the server status in a cluster:

  Sign in to Cisco Unity Connection Serviceability.

  Expand Tools and select Cluster Management.

  Check the server status in a cluster.

  In addition to this, confirm the running state of database replication using the CLI command show cuc cluster status.

Note After confirming the status of publisher server as Primary and subscriber server as Secondary, start the upgrade process first on publisher server and then on subscriber server.

- Before upgrading to Unity Connection Release 15, rename the notification templates if created with the below mentioned names.

  Default_Missed_Call

  Default_Missed_Call_With_Summary

  Default_Scheduled_Summary

  Default_Voice_Message_With_Summary

  Default_Dynamic_Icons

  Default_Actionable_Links_Only

  If not renamed the mentioned notification templates gets replaced with default notification templates of release 15.

- Before upgrading to Unity Connection Release 15, make sure the display name of default notification devices is not changed for any of the user. If changed then update notification devices to the default name.

  To check the users whose default notification device name is changed, execute below query:

```
run cuc dbquery unitydirdb SELECT COUNT(*) AS num_sys_notdevices, USR.alias,
ND.subscriberobjectid FROM tbl_notificationdevice AS ND INNER JOIN vw_user USR ON
ND.subscriberobjectid = USR.objectid WHERE ((ND.devicename IN ('Home Phone', 'Work
Phone', 'Mobile Phone', 'Pager', 'SMTP') AND ND.displayname = ND.devicename) OR
(ND.devicename='HTML' AND ND.displayname IN ('HTML', 'HTML Missed Call', 'HTML Scheduled
 Summary'))) GROUP BY ND.subscriberobjectid, USR.alias HAVING COUNT(*) != 8
```

- Initiate a pre upgrade test before starting the upgrade process using the CLI command

  run cuc preupgrade test

- If you have legacy and PLM based licenses in earlier releases, you must migrate the licenses to Cisco Smart Software Licensing before upgrade to Unity Connection Release 15. For more information on Cisco Smart Software Licensing flow in Unity Connection see Managing Licenses chapter of *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 15*.

Caution For successful upgrade of Unity Connection from 12.0(1) to any higher releases, make sure the system does not exist in Enforcement mode before upgrade.For more information on Enforcement mode, see Enforcement Policy on Unity Connection section.

- Unity Connection Release 15 supports ESXi version of 7.0 U3. For more information on Virtual Hardware settings, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html.
- The Exchange 2003, 2007, 2010, 2013 is end of support now. Therefore, it is recommended to delete the Unified Messaging Service configured with Exchange 2003 or 2007 or 2010 or 2013 while upgrading to Unity Connection Release 15 or later. Now, create a new Unified Messaging Service with supported Exchange version 2016 or 2019 to avoid any issues while using Unified Messaging Services.

Note In the upgrade logs, it is 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.

Upgrade Considerations with FIPS Mode

If you are performing upgrade with FIPS enabled Unity Connection Release to 15 and later, you must consider the below limitations for a successful upgrade:

- Before upgrading Unity Connection using FIPS-enabled mode, make sure that the security password length is greater than or equal to 14 characters to meet FIPS compliance.
- In Unity Connection Release 15, the IPsec policies with DH group key values 1, 2 or 5 are disabled. If you are upgrading Unity Connection to Release 15 with FIPS enabled and IPse configured, then you must perform any one of the given procedure for successful upgrade to Unity Connection 15
  - Delete the previously configured IPsec policies and perform the upgrade. After the upgrade is complete, reconfigure the IPsec policies with DH groups 14–18.
  - Install the **ciscocm_ipsec_groupenhancement_fips_<version>.cop** COP file that supports DH groups 14–18, reconfigure the IPsec policies and then perform an upgrade.

Note If you disable the FIPS mode after installing the COP file, the IPsec configuration page does not appear.

- If you are upgrading Unity Connection which has IPsec configured using a certificate-based authentication with self-signed certificate, then you must reconfigure the IPsec policy with a CA-signed certificate foe a successful upgrade.
- In FIPS mode, if you have configured Unified Messaging with NTLM web authentication mode then you must select a Basic authentication mode before upgrading Unity Connection to 15 and later. NTLM web authentication mode is no longer supported.
- If you are upgrading from any release of Unity Connection 12.5 in FIPS mode to Unity Connection 15 and later, make sure to install COP File **ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512** on both nodes of cluster before upgrade.

For more information on FIPS mode, see "FIPS Compliance in Cisco Unity Connection" chapter of *Security Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.

Task list to Upgrade to Unity Connection Shipping Version 15

Do the following tasks to upgrade an Unity Connection server:

1. If you are running the current version of Unity Connection on a physical server then you must replace it with a virtual server. See the Migrating a Physical Server to a Virtual Machine.

   If you are already running the current version on a virtual server, make sure it is compatible with the upgraded version. See the Cisco Unity Connection 15 Supported Platform List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/supported_platforms/b_15cucspl.html.

   Note If you are performing an L2 upgrade, make sure that the Platform SOAP services are running on both the Unity Connection servers to successfully upgrade using Prime Collaboration Deployment. SOAP services can be enabled on both the servers using Cisco Unified Serviceability page. For more information on PCD, see the Cisco Prime Collaboration Deployment Administration Guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

2. If you are upgrading during non business hours, run the following command on the standalone server or the publisher server to speed up the upgrade process:

   utils iothrottle disable

   If you are upgrading during a maintenance window, you can speed up the upgrade by disabling the throttling. This decreases the time required to complete the upgrade but affects Unity Connection performance.

   Caution You cannot disable throttling during the upgrade process. If you want to disable the throttling process, you must first stop upgrade, disable throttle, and restart the Unity Connection server. Once the server is active again, begin the upgrade process.

3. Migrate all the licenses (legacy and PLM based) before you upgrade to Unity Connection 15 server. For more information, see the Migrating Licenses section.

4. Confirm if you require COP file for the upgrade process and download file from https://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm
5. Apply the COP file using the steps listed in the Applying COP file from a Network Location.
6. Follow the upgrade process on the standalone server:
   - (RU upgrades only) Upgrade the server by performing the steps mentioned in the Upgrading the Unity Connection Server section. The server automatically switches to the new version after completing the upgrade.
   - (L2 upgrades only) Upgrade the server using the steps mentioned in the Upgrading the Unity Connection Server section. Switch to the upgraded software to complete the upgrade process following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software section.
7. Follow the upgrade process on the Unity Connection cluster:
   - (RU upgrades only) Upgrade the publisher server following the steps mentioned in the Upgrading the Unity Connection Server section. The server automatically switches to the new version after completing the upgrade.

     Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server section. The server automatically switches to the new version after completing the upgrade.
   - (L2 upgrades only) Upgrade the publisher server using the steps mentioned in the Upgrading the Unity Connection Server section.

Caution In case of L2 upgrade of a cluster, do not restart or perform switch version on the publisher server before completing the upgrade on subscriber server otherwise cluster does not function properly.

Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server section.

Switch to the upgraded software first on the publisher server and then on the subscriber server following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software section.

8. Confirm that publisher server has Primary status and subscriber server has Secondary status.
9. After successful upgrade to Unity Connection 15, the product remains in Evaluation Mode until you register the product with CSSM or satellite.
10. If you are performing an upgrade from a FIPS enabled Unity Connection Release to Unity Connection 15, make sure to follow the steps for regenerating certificates before using any pre-existing telephony integrations. To learn how to regenerate certificates, see the Regenerating Certificates for FIPS section of the "FIPS Compliance in Cisco Unity Connection" chapter in *Security Guide for Cisco Unity Connection Release 15,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.
11. If Secure SIP call is configured on the system using SIP Integration then after successful upgrade, generate and upload RSA based Tomcat certificates. To learn how to regenerate certificates, see Settings for RSA Key Based certificates section of the "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter in *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 15,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucm_sip/b_15cucintcucmsip.html.

Note Verify that the value entered in **X.509 Subject Name** field on SIP Trunk Security Profile Configuration page of Cisco Unified Communication Manager is the FQDN of the Unity Connection server

12. Cisco Unity Connection supports HAProxy which frontends all the incoming web traffic into Unity Connection offloading Tomcat. HAProxy sends the request internally to Tomcat via HTTP. For information on new ports which should be opened after successful upgrade, see chapter IP Communications Required by Cisco Unity Connection in *Security Guide for Cisco Unity Connection Release 15,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.

13. If Next Generation Security over HTTPS interface is configured on the system then after successful upgrade to Unity Connection 15, the configured settings of HTTPS ciphers get reset. You must reconfigure the HTTPS ciphers on Enterprise Parameter page of Cisco Unity Connection Administration and restart the Tomcat service.

Note In case of a cluster, you must configure the HTTPS ciphers on publisher server and restart the Tomacat service on each node to reflect the changes.

14. If Specific License Reservation(SLR) mode is enabled on the system, then after successful upgrade to Unity Connection Release 15, you must return all reserved licenses to Cisco Smart Software Manager(CSSM) and reconfigure SLR with new version licenses. For more information on configuration of Specific License Reservation in Unity Connection, see the Configuring Specific License Reservation in Unity Connection section of the "Managing Licenses" chapter in *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html.

15. Cisco Unity Connection supports SAML-based Single Logout (SLO). The SLO allows you to log out simultaneously from all sessions of a browser that you have signed in using Single Sign-on (SSO). SLO does not close all the running sessions at the same time. If SAML SSO mode is enabled with Microsoft ADFS 2.0 configuration on the system, then after successful upgrade to Unity Connection Release 15 you must follow steps mentioned in section SAML-Based Single Logout (SLO) of *Quick Start Guide for SAML SSO Access* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/quick_start/guide/b_15cucqssamlsso.html.

16. To avoid upgrade related issues it is recommended to run Pre Upgrade COP file before upgrade. The COP file will run a series of tests to check the pre-upgrade health and connectivity of your system. If the COP file highlights issues that need to be addressed, fix them before proceeding with the upgrade. After sucessful upgrade it is recommended to run Post Upgrade COP file to verify the configuration of system. Download the COP files from http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm.

Caution *(Applicable to 12.5SU1, 12.5SU2, 12.5SU3 releases only)* For upgrading Unity Connection to release 15, Pre and Post Upgrade COP files should be installed via CLI only.

17. If you are creating a new Intrasite link or if there is any existing Intrasite link between two nodes of Unity Connection in FIPS mode with one node on 15 release and other node on any release lower than

15, then only message delivery between two nodes will work. Object(users, system distribution lists if applicable, partitions, search spaces and Unity Connection locations) synchronization is not supported. For object synchronization to work, you must upgrade all the Unity Connection nodes in network to 15 release.

18. After successful upgrade to Unity Connection 15, if you need to perform rollback of server from 15 to any older release then you must re-register the product with CSSM or satellite using a registration token for successful functioning of Smart Licensing as applicable to the release.

19. If Secure SMTP is enabled on the system, then after successful upgrade to Unity Connection Release 15 you must reconfigure the Secure SMTP feature using Cisco Unity Connection Administration. For more information, see Configure SMTP Client Communication section of the chapter "Messaging" of the System Administration Guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html.

20. CUNI Subscriptions will be removed from Cisco Unity Connection server database, if you perform a refresh upgrade to Unity Connection 15. Make sure to perform re-subscription after successful upgrade of the cluster.

21. If you are performing upgrade to Unity Connection 15 from any of the older release, make sure to reconfigure permissions on Azure Portal after sucessful upgrade. To learn how to reconfigure the permissions, see Step4g of the section "Task List for Configuring Unified Messaging with Office 365" of the chapter "Configuring Unified Messaging" of the *Unified Messaging Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/unified_messaging/guide/b_15cucumgx.html.

Upgrading the Unity Connection Server

Do the following steps to upgrade a standalone server or a cluster. In case of a cluster, follow the steps first on the publisher server and then on the subscriber server.

Step 1 Do any one of the following:

- Copy the ISO file to a folder on an FTP or SFTP server that the Unity Connection server can access.
- Insert the DVD with the ISO file of the Unity Connection server that you want install into the disk drive of the server.

Step 2 Sign in to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, select **Install/Upgrade**.

Step 4 *(Applicable only for subscriber server) (Optional)* On the Software Installation/Upgrade page, check the **Use download credentials from Publisher** check box to use the source configuration provided for the publisher server and move to Step 13.

Step 5 In the **Source** field, select any one of the following:

- **Remote Filesystem**: Select this option to upgrade from remoter server and follow this procedure.
- **DVD/CD**: Select this option to upgrade from disk drive and move to Step 11.
- **Local Filesystem**: Select this option to use the previously downloaded ISO or COP files for the upgrade.

Step 6 In the **Directory** field, enter the path of the folder that contains the upgrade file.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the upgrade file is in the upgrade folder, you must enter /upgrade).

If the upgrade file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

Step 7 In the **Server** field, enter the server name or IP address.

Step 8 In the **User Name** field, enter the alias that is used to sign in to the remote server.

Step 9 In the **User Password** field, enter the password that is used to sign in to the remote server.

Step 10 In the **Transfer Protocol** field, select the applicable transfer protocol.

Step 11 In the **SMTP Server** field, enter the IP address of the SMTP server.

Step 12 In the **Email Destination** field, enter your email address along with the SMTP server.

Step 13 Select **Next**.

Step 14 Select the upgrade version that you want to install and select **Next**.

The upgrade file is copied to the hard disk of the Unity Connection server. When the file is copied, a screen displaying the checksum value appears.

Step 15 Verify the checksum.

Step 16 On the next page, monitor the progress of the upgrade.

Caution If you loose your connection with the remote server or close your browser during this step, you may see the following warning when you try to view the Software Installation/Upgrade page again:

Warning: Another session is installing software, click Assume Control to take over the installation. To continue monitoring the upgrade, select Assume Control.

To continue monitoring the upgrade, select Assume Control.

Step 17 Select **Next**.

During the initial phase of upgrade, the Installation Log text box in Cisco Unified Operating System Administration is updated with the information on the progress of the upgrade. To confirm the completion of upgrade, open the console of the Unity Connection server and make sure that a message indicating the completion of upgrade appears on the screen along with the login prompt.

Step 18 Select **Finish**.

Step 19 To verify if the upgrade is successful, run the following CLI commands:

- show cuc version: Displays the version of Unity Connection server in both active and inactive partitions. The upgraded Unity Connection version is in the inactive partition and old version is in the active partition.
- utils system upgrade status: Displays the status of the upgrade that you performed. This command should display the message for successful upgrade along with the upgraded version.

Switching to the Upgraded Version of Unity Connection Software

After completing the upgrade process, you can select either manual switch version or automatic switch version. The method that you choose depends on the type of upgrade that you are doing. During the upgrade process, the wizard prompts you to choose whether to switch the software version automatically by rebooting to the upgraded partition, or whether to switch the version manually at a later time.

Automatic Switching

The table below lists the automatic switching method to use for each type of upgrade.

Upgrade Type	When prompted, choose...	Result
L2 Upgrade	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	When you choose this option, the system reboots to the new software version.
Refresh Upgrade	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	Choose this option to use the new upgraded software version immediately following the upgrade. **Note** Option "Do not reboot after upgrade" is not supported on GUI and if selected, the system will still reboot and pick the upgraded version.

You can perform the switch version running the CLI command utils system switch-version. The system automatically reboots after the switch version.

Manual Switching

If you select not to automatically switch to the upgraded partition at the end of the upgrade, do the following procedure when you are ready to switch partitions.

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the **Settings** menu, select **Version**.

Step 3 On the Version Settings page, select **Switch Versions**, to start the following activities:

- Unity Connection services are stopped.
- Data from the active partition is copied to the inactive partition. Note that the messages are stored in a common partition, therefore they are not copied.
- The Unity Connection server restarts and switches to the newer version.

Applying COP file from a Network Location

Step 1 Copy the Cisco Option Package (.cop) file on an FTP or SFTP server that the server can access.

Step 2 Sign in to Cisco Unified Operating System Administration.

If you are upgrading the subscriber server in a Unity Connection cluster, type the following address to access Cisco Unified Operating System Administration:

http://<Unity Connection_servername>/cmplatform

Step 3 From the Software Upgrades menu, select Install/Upgrade.

Step 4 On the Software Installation/Upgrade page, in the Source field, select Remote Filesystem.

Step 5 In the Directory field, enter the path to the folder that contains the .cop file.

If the .cop file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the .cop file is in the cop folder, you must enter /cop).

If the .cop file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

Step 6 In the Server field, enter the server name or IP address.

Step 7 In the User Name field, enter the alias that is used to sign in to the remote server.

Step 8 In the User Password field, enter the password that is used to sign in to the remote server

Step 9 In the Transfer Protocol field, select the applicable transfer protocol and select Next.

Step 10 Select the software that you want to install, and select Next.

The .cop file is copied to the virtual hard disk on Unity Connection server. When the file is copied, a screen displays the checksum value.

Step 11 Verify the checksum and select Next to begin the installation.

During the upgrade, the value of the Status field is Running. When the upgrade process is complete, the value of the Status field changes to Complete.

Note
- All command-line interface sessions are terminated automatically.
- The Cisco Tomcat Service can take several minutes to restart automatically.

Step 12 Sign out from the Cisco Unified Operating System Administration application.

Step 13 Run the CLI command utils service list to confirm that the Cisco Tomcat service is in the Running state.

Rollback of Unity Connection

After upgrading the Unity Connection version, you can rollback to the software version that was running before the upgrade by switching to the software version on inactive partition.

Caution If you revert to the version on the inactive partition in case of RU upgrade rollback from 15 to 14,12.x or 11.x or 10.x versions, you cannot later switch to the newest version again. Instead, you must reinstall the upgrade as documented in this guide.

Important Considerations for Rollback

1. Do not make any configuration changes during the rollback because the changes are lost after the rollback.
2. In an cluster setup, do not switch versions on both the first and second servers at the same time. Perform switch version on the second server only after you have switched versions on the first server.
3. Users and mailbox stores that were added after the upgrade, no longer exist after you rollback to the version on inactive partition. The new users and mailbox stores are deleted.
4. All messages are preserved but in Refresh Upgrades, if a rollback is performed then any messages left for existing users on the new version will be lost. While in Level 2 Upgrades, any messages left for existing users on the new version will be retained, even if a rollback is done.
5. If you moved mailboxes from one mailbox store to another after upgrading, those mailboxes are moved back to the mailbox stores they were in before the upgrade.
6. A future delivery folder is created for users to mark messages for future delivery. If you revert to a version that supports future delivery but the future delivery folder has not been created for the user as yet, the messages in the future delivery folder for the new version are moved to the undeliverable messages folder.
7. (Unity Connection 8.5 and earlier only) If a user rollbacks to Unity Connection version 8.5 or earlier from a current version that is 8.6 and higher, then following limitations are faced:
   - No voice messages are left after the rollback.
   - No administrator settings are preserved after the rollback.
8. No administrator settings are preserved after the rollback.
   a. Revert to the Guest Operating System version as earlier (before upgrade).
   b. Modify the network adapter to the adapter type as earlier (if you changed after upgrade).

Rollback Scenarios

You can revert a single Unity Connection server or a cluster to the version on inactive partition.

To rollback a Unity Connection cluster, you should rollback both the servers, first the publisher and then the subscriber. After the successful rollback of both the publisher and subscriber servers, reset the replication between the two servers running the following CLI commands:

Stop the replication on subscriber server with the CLI command utils dbreplication stop.

Stop the replication on publisher server with the CLI command utils dbreplication stop.

Reset the replication running the CLI command utils dbreplication reset all on the publisher server.

After the reset of replication between the two servers, check the cluster status running the CLI command show cuc cluster status utils system restart on both publisher and subscriber.

Rollback a Unity Connection Server to the Version in the Inactive Partition

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, select Version and the Version Settings window displays.

Step 3 Select the Switch Versions option. After you confirm that you want to restart the system, the system restarts that might take up to 15 minutes.

Step 4 Follow the given steps to confirm that the switch version is successful:

a. Sign in to Cisco Unified Operating System Administration.

b. In the Settings menu, select Version. The Version Settings window displays the product version.

c. Confirm that the active partition runs the correct version of Unity Connection server and all critical services are in the Running state.

d. Sign in to Cisco Unity Connection Administration and confirm that the configuration data exists.