



Upgrades

- [Upgrade Procedures, on page 1](#)
- [Supported Upgrade and Migration Paths, on page 1](#)
- [Requirements and Limitations, on page 5](#)

Upgrade Procedures



Note If your pre-upgrade version is Release 11.5(1)SU9 of Cisco Unified Communications Manager and the IM and Presence Service, you cannot upgrade to Releases 12.0(x), 12.5(1), or 12.5(1)SU1. The minimum Release that you can upgrade to is 12.5(1)SU2.

For detailed procedures on how to upgrade your system, see the [Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5\(1\)](#).

Supported Upgrade and Migration Paths

Use the following tables to determine whether you can upgrade or migrate from your currently installed version, and which of the supported upgrade methods are available to you:

- Direct upgrades using either the Cisco Unified CM OS Admin interface or the Cisco Prime Collaboration Deployment (PCD) Upgrade task
- Migrations using the PCD Migration task

Deployments on Cisco Media Convergence Servers Hardware

You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. The tables below list the supported migration paths for deployments that are currently running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations.



Note The tables below list the upgrade paths supported for MCS 7800 Series servers, with the following exceptions:

- MCS 7816-C1 for Business Edition 3000 (BE3000)
- MCS 7828 for Business Edition 5000 (BE5000)

PCD migrations are not supported for BE3000 and BE5000 deployments. We recommend a fresh installation for upgrades from these products.

Table 1: Unified Communications Manager Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
6.1(5)	11.5(x)	PCD Migration
7.1(3) and 7.1(5)	11.5(x)	PCD Migration
8.x	11.5(x)	PCD Migration
9.x	11.5(x)	PCD Migration

Table 2: Cisco Unified Presence and IM and Presence Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration
IM and Presence 9.x	11.5(x)	PCD Migration

Deployments on Virtual Machines

The tables below list the supported upgrade and migration paths for Cisco Unified Communications Manager and IM and Presence Service deployments that are currently running on virtual machines. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V). Service Updates (SU) within each path are supported, unless otherwise indicated.

Table 3: Unified Communications Manager Releases Installed on Virtual Machines

From	To	Supported Method
8.6(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh) PCD Migration PCD Upgrade (Direct Refresh)
9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)

From	To	Supported Method
9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh) Cisco Unified OS Admin (Direct Refresh)
10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard)
10.5(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)
11.0(1)	11.5(x)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)
11.5(x)	11.5(y)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)

Table 4: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
CUP 8.6(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh)
IM and Presence 9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
IM and Presence 9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh) Cisco Unified OS Admin (Direct Refresh)
IM and Presence 10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) PCD Upgrade (Direct Standard)

From	To	Supported Method
IM and Presence 10.5(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)
IM and Presence 11.0(1)	11.5(x)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)
IM and Presence 11.5(x)	11.5(y)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)

Upgrade Path Restrictions for Release 11.5(x)

Upgrade and migration paths generally support the Service Updates (SU) within each path; however, there are some exceptions for specific SU releases. The table below lists the exceptions for upgrades and migrations to Cisco Unified Communications Manager Release 11.5(x).

Table 5: Restrictions to Supported Upgrade and Migration Paths, Cisco Unified Communications Manager Release 11.5(x)

From	To	Description
10.5(2)SU5	11.5(1.10000-6) through 11.5(1.120xx)	Path is unsupported. For these releases, upgrade to 11.5(1)SU2 instead.

COP Files Required for Upgrades to Release 11.5

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Admin interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool. If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.

Table 6: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(x)

From	To	Upgrade Type
8.6(x)	11.5(x)	Refresh upgrade. Required COP files: <ul style="list-style-type: none"> ciscocm.version3-keys.cop.sgn Optional COP files: <ul style="list-style-type: none"> ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) ciscocm.free_common_space_v<latest_version>.cop.sgn

From	To	Upgrade Type
9.1(x)	11.5(x)	Refresh upgrade. Required COP files: <ul style="list-style-type: none"> ciscocm.version3-keys.cop.sgn Optional COP files: <ul style="list-style-type: none"> ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5(y)	Standard upgrade; no COP file required.

Table 7: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	11.5(x)	Refresh upgrade. Requires the following COP files: <ul style="list-style-type: none"> cisco.com.cup.refresh_upgrade_v<latest_version>.cop ciscocm.version3-keys.cop.sgn

Table 8: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	11.5(x)	Refresh upgrade. Requires the following COP file: <ul style="list-style-type: none"> ciscocm.version3-keys.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5(y)	Standard upgrade; no COP file required.

Requirements and Limitations

This section contains requirements and limitations to consider when upgrading your system.

Upgrade Requirements with Standalone Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, SU6, SU7, SU8, SU9., SU10, and SU11 are compatible with Cisco Prime License Manager Release 11.5(1)SU2 or higher. If you are deploying a standalone Cisco Prime License Manager, make sure that your Prime License Manager version is a minimum release of 11.5(1)SU2. Otherwise, Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these Unified Communications Manager releases and you are running a standalone version of Prime License Manager, upgrade your Prime License Manager instance to 11.5(1)SU2 or higher before you upgrade Unified Communications Manager.



Note With co-resident Prime License Manager deployments, Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

Cisco Jabber Users Should be Logged Out During Upgrade

When upgrading the IM and Presence Service, it's best to ensure that all Cisco Jabber users are logged out during the upgrade. The more Cisco Jabber user activity you have, the greater the likelihood that you will receive an error that requires administrator intervention such as a Presence status sync error.

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades

If you are using the **utils system upgrade** CLI command to upgrade IM and Presence Service nodes, you must use the default OS admin account, as opposed to a user with administrator privileges. Otherwise, the upgrade will not have the required privilege level to install essential services, thereby causing the upgrade to fail. You can confirm the account's privilege level by running the **show myself** CLI command. The account must have privilege level 4.

Note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. See your ISO Readme file for details on your specific ISO file. For-up-to date information on this limitation, see [CSCvb14399](#).

Rolling Back to Previous Versions

If you run into any upgrade issues and you need to roll back to a previous version, you must roll back both the Unified Communications Manager and the IM and Presence Service installations to the previous version or you will have a non-supported version mismatch.

It's not supported to roll back the Unified Communications Manager version and leave the IM and Presence Service version at 11.5(1)SU2. Similarly, it's not supported to roll back the IM and Presence Service version and leave the Unified Communications Manager version at 11.5(1)SU2.

Upgrading with FIPS Mode Enabled

For Release 11.5(x), Unified Communications Manager and IM and Presence Service do not support RSA certificates with key-sizes that are less than 2048 bits when FIPS mode is enabled. This affects server certificates and LSCs.

If you are upgrading to Release 11.5(x) with FIPS mode enabled and you are using RSA key-sizes that are less than 2048 bits on your current version, then you can carry out one of the following items to resolve the problem.

You can either:

- Regenerate the effected certificates before you upgrade if your current version supports key-sizes of 2048 bits, or
- Regenerate the effected certificates after you upgrade to Release 11.5(x).



Note If you choose this option, then secure connections are not allowed to use the effected certificates until they have an RSA key-size of 2048 bits or greater.

Upgrades with Mixed Mode Enabled Require an Encryption License

This release requires that you have an encryption license installed in order to run Unified Communications Manager in mixed mode. If you are upgrading from an earlier release of Unified Communications Manager, and cluster security is set to mixed-mode, you must obtain an encryption license and install it in Cisco Prime License Manager.

If you upgrade from an earlier release with mixed-mode enabled, but you do not have an encryption license installed, a warning message on the encryption license requirement displays on the user interface immediately following the upgrade. You will also receive the **CiscoSystemEncryptionNotAllowed** alert. Your system will continue to operate in mixed-mode, but you will be unable to update the CTL file and will continue to receive this alert until you either install an encryption license or move the cluster security setting back to non-secure mode. We recommend that you install the encryption license at the earliest to ensure that you can continue to run mixed mode without any disruption.

If you were not running mixed-mode prior to the upgrade, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Unified Communications Manager, and a sync has been completed.

Ordering and Installing License Files

The following table describes how to update your system with an encryption license.

Table 9: Updating your System with an Encryption License

Step	Task	Description
Step 1	Obtain an ENC PAK license file.	Use the CUCM-PLM-ENC-K9= part number to order encryption licenses via the Product Upgrade Tool at https://tools.cisco.com/gct/Upgrade/jsp/index.jsp . For further information on ordering licenses, see the Cisco Unified Communications Solutions Ordering Guide . Note If you are using multiple instances of Cisco Prime License Manager in your deployment, you must order a separate encryption license for each Prime License Manager instance.
Step 2	Install the encryption license file in Cisco Prime License Manager.	Follow the "Upgrade Existing Licenses" procedure in the Cisco Prime License Manager User Guide, Release 11.5(1)SU2 .
Step 3	Synchronize licenses.	In Cisco Prime License Manager, select the Product Instances tab and click Synchronize licenses . For additional detail, see the <i>Cisco Prime License Manager User Guide, Release 11.5(1)SU2</i> .

Database Migration Required for Upgrades with Microsoft SQL Server

If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database. This is required due to enhanced data type support in this release. If you don't migrate your database, schema verification failure will occur on the existing SQL Server database and services that rely on the external database, such as persistent chat, will not start.

After you upgrade your IM and Presence Service, use this procedure to create a new SQL Server database and migrate data to the new database.



Note This migration is not required for Oracle or PostgreSQL external databases.

Before You Begin

The database migration is dependent on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

Table 10:

Step	Task
Step 1	Create a snapshot of your external Microsoft SQL Server database.
Step 2	<p>Create a new (empty) SQL Server database. For details, see the following chapters in the <i>Database Setup Guide for the IM and Presence Service</i>:</p> <ol style="list-style-type: none"> 1. "Microsoft SQL Installation and Setup"—See this chapter for details on how to create your new SQL server database on your upgraded IM and Presence Service. 2. "IM and Presence Service External Database Setup"—After your new database is created, refer to this chapter to add the database as an external database in the IM and Presence Service.
Step 3	<p>Run the System Troubleshooter to confirm that there are no errors with the new database.</p> <ol style="list-style-type: none"> 1. From Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter. 2. Verify that no errors appear in the External Database Troubleshooter section.
Step 4	<p>Restart the Cisco XCP Router on all IM and Presence Service cluster nodes:</p> <ol style="list-style-type: none"> 1. From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services. 2. From the Server menu, select an IM and Presence Service node and click Go. 3. Under IM and Presence Services, select Cisco XCP Router, and click Restart.
Step 5	<p>Turn off services that depend on the external database:</p> <ol style="list-style-type: none"> 1. From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services. 2. From the Server menu, select an IM and Presence node and click Go. 3. Under IM and Presence Services, select the following services: <ul style="list-style-type: none"> Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver 4. Click Stop.
Step 6	<p>Run the following script to migrate data from the old database to the new database <code>MSSQL_migrate_script.sql</code>.</p> <p>Note Contact Cisco TAC to obtain a copy of this script</p>

Step	Task
Step 7	<p>Run the System Troubleshooter to confirm that there are no errors with the new database.</p> <ol style="list-style-type: none"> From Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter. Verify that no errors appear in the External Database Troubleshooter section.
Step 8	<p>Start the services that you stopped previously.</p> <ol style="list-style-type: none"> From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services. From the Server menu, select an IM and Presence node and click Go. Under IM and Presence Services, select the following services: <ul style="list-style-type: none"> Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver Click Start.
Step 9	<p>Confirm that the external database is running and that all chat rooms are visible from a Cisco Jabber client. Delete the old database only after you're confident that the new database is working.</p>

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the 11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system, do the following:

Procedure

Step 1 Disable Push Notifications

Follow these steps:

- From Cisco Unified CM Administration, choose **Advanced Features > Cisco Cloud Onboarding**.
- Uncheck the following check boxes:
 - **Enable Push Notifications**
 - **Send Troubleshooting information to the Cisco Cloud**
 - **Send encrypted PII to the Cisco Cloud for troubleshooting**

c. Click **Save**.

Step 2 Enable Push Notifications for this release.

For the full onboarding process, see the "Push Notifications Configuration Task Flow" in the [Deploying Push Notifications for Cisco Jabber on iPhone and iPad](#) guide.
