



Understanding Upgrades and Migrations

- [Upgrade and Migration Overview, on page 1](#)
- [Upgrade Methods, on page 1](#)
- [Upgrade and Migration Tools, on page 3](#)
- [Export Restricted and Export Unrestricted Software, on page 3](#)

Upgrade and Migration Overview

This document will guide you through the process of determining what you need to upgrade and where to find the information that you need to complete the upgrade process.

Upgrade Methods

There are two main methods of upgrading Unified Communications Manager and Instant Messaging and Presence:

- [Direct Upgrades, on page 1](#)
- [Migrations, on page 3](#)

Direct Upgrades

A direct upgrade is when the new software will be installed on the same physical server and the same virtual server where the currently installed version is running. Direct upgrades allow you to upgrade from your current release to the latest release without the need to upgrade to an intermediate software version. It is a single upgrade rather than a multi-hop upgrade.

There are two types of direct upgrade:

- standard upgrades
- refresh upgrades

Standard upgrades are upgrades that do not require upgrades to the embedded operating system. You can install upgrade software on your server while the system continues to operate.

Refresh upgrades are required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the embedded operating system changes between the version you are upgrading from and the version that you are upgrading to.

The application automatically determines whether you need to perform a standard upgrade or a refresh upgrade.

Standard upgrades

Standard upgrades are upgrades that do not require upgrades to the operating system. You can install upgrade software on your server while the system continues to operate.

For standard upgrades, you install the upgrade software as an inactive version. The system continues to function normally while you are installing the software. When the upgrade is complete, you can choose to automatically reboot the system to the upgraded software or you can manually switch to the new software at a later time. When you reboot to the new software, the old software version remains on the system. This allows you to revert to the old version in the unlikely event of issues with the new software. During an upgrade your configuration information migrates automatically to the upgraded version.



Note

You can only make any provisioning changes to the database on the active software. The database for the inactive software is not updated. If you make changes to the database after an upgrade, you must repeat those changes after switching to the new software.



Note

See *Resuming a Failed Upgrade* section of the *Troubleshooting* chapter for more details.

Refresh upgrades

Refresh upgrades are required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the embedded operating system changes between the version you are upgrading from and the version that you are upgrading to. Refresh upgrades require multiple reboots during installation to upgrade the underlying operating system, causing a temporary server outage while the software is installed. The duration of this outage will depend on your configuration and the size of the database.



Note

You must perform all refresh upgrades during a maintenance window because the system will not be available during the upgrade.

For refresh upgrades, the upgrade wizard allows you to choose whether or not to automatically run the new upgraded software when the upgrade completes. If you select not to run the new software, the system will reboot to the old software version when the upgrade is complete and you can manually switch to the new software at a later time.

If for any reason you decide to revert to the prior software version, you can switch versions to the older version of the software. This switch version requires a reboot. Be aware that any configuration changes that you made after upgrading the software will be lost.

Migrations

A migration is an upgrade where the new software will be installed on a different hardware system or virtual machine than the currently installed version. For example, you need to use the migration method in the following situations:

- your currently installed version is running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware and you are upgrading to release that will run on a virtual machine.
- your currently installed version is running on a virtual machine and you need to move to a new virtual machine.
- you are upgrading to Unified Communications Manager from another application, such as Unified Communications 300 (UC300) Series, Unified Communications (UC500) Series, or certain Cisco Business Edition products.

Upgrade and Migration Tools

Following are tools available for upgrading or migrating Unified Communications Manager and Instant Messaging and Presence:

- **Unified CM OS Administration:** This interface is part of Unified Communications Manager and you can use it to perform direct upgrades.
- **Prime Collaboration Deployment (PCD):** This is a management tool for Unified Communications (UC) applications, which supports a range of tasks. You can perform direct upgrades using the PCD Upgrade task, and you can perform migrations using the PCD Migration task.

Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and Instant Messaging and Presence supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.

**Note**

Unrestricted versions of software are intended only for a very specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.
- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.
- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.
- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and Instant Messaging and Presence in the same cluster must either all be in unrestricted mode or all be in restricted mode.

- IP phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

**Note**

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

For all Graphical User Interfaces (GUIs) and Command Line Interfaces (CLIs), the Administrator can view the product version (restricted or export unrestricted).

The following table describes the GUI items that are not available for the export unrestricted version of Instant Messaging and Presence.

GUI Item	Location	Description
Cisco Unified CM Administration		
VPN Configuration	Advanced Features > VPN	This menu and its options are not available.
Phone Security Profile Configuration	System > Security > Phone Security Profile	The Device Security Mode is set to Non Secure and is not configurable.
Cisco Unified CM IM and Presence Administration		
Security Settings	System > Security > Settings	<ul style="list-style-type: none"> • You cannot check the Enable XMPP Client to IM/P Service Secure Mode setting. • You cannot check the Enable XMPP Router-to-Router Secure Mode setting. • You cannot check the Enable Web Client to IM/P Service Secure Mode setting. • The option to set SIP intra-cluster Proxy-to-Proxy Transport Protocol to TLS have been removed.
Service Parameter Configuration for Cisco SIP Proxy service	System > Service Parameters and choose Cisco SIP Proxy as the Service	<ul style="list-style-type: none"> • All TLS options have been removed for the Transport Preferred Order parameter. • The TLS option have been removed from the SIP Route Header Transport Type parameter.

GUI Item	Location	Description
SIP Federated Domains	Presence > Inter-domain Federation > SIP Federation	When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode.
XMPP Federation Settings	Presence > Inter-domain Federation > XMPP Federation > Settings	You cannot configure the security mode; It is set to NO TLS .
Proxy Configuration Settings	Presence > Routing > Settings	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.

