Upgrade Planning

This chapter provides the following information:

- Requirements and Limitations, on page 1
- Supported Upgrade Paths, on page 7
- Licensing Requirements, on page 11
- Export Restricted and Export Unrestricted Software, on page 12

Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Unified Communications Manager or IM and Presence Service serivce.

Caution Do not modify any of the IM and Presence Service Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service Service upgrade process automatically updates these entries on the Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service Service and Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Unified Communications Manager and IM and Presence Service Service clusters.

Limitations

This section describes the limitations that apply when you install or upgrade Unified Communications Manager or the IM and Presence Service Service.

Subnet Limitations

Do not install Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices.

Cluster Size

The number of Unified Communications Manager subscriber nodes in a cluster cannot exceed 4 subscriber nodes and 4 standby nodes, for a total of 8 subscribers. The total number of servers in a cluster, including the Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

The maximum number of IM and Presence Service nodes in a cluster is 6.

For more information, see *"Cisco Collaboration Solutions Design Guidance"* at http://www.cisco.com/go/ucsrnd

Support for Intercluster Peers

The IM and Presence Service supports intercluster peers to clusters that are running different software versions. To find the interdomain federations that are supported, see the "Supported Integrations" chapter in the Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service .

Parameter Settings

With the merging of Cisco Unified Communications Manager and IM and Presence Service, enterprise and service parameters are now shared between nodes in a cluster. As such, both types of nodes use the same settings for enterprise and cluster-wide parameters. You need to be aware that not all parameter settings are retained during an upgrade to Release 10.0(1). All enterprise parameters and cluster-wide service parameters that are common to both Cisco Unified Communications Manager and IM and Presence Service retain the value specified on Cisco Unified Communications Manager only, with one exception. The User Assignment Mode parameter is the only enterprise parameter that is retained during upgrade. Service parameters that apply to IM and Presence only are retained after an upgrade.

Cisco recommends that before you begin an upgrade, you make a note of parameter settings and evaluate the best settings for the combined cluster. This will allow you to easily configure those settings after the upgrade is complete.

Network Requirements

This section lists the requirements that your network must meet before you can deploy Unified Communications Manager and the IM and Presence Service.

IP Address Requirements

A complete collaboration solution relies on DNS in order to function correctly for a number of services and thus requires a highly available DNS structure in place. If you have a basic IP telephony deployment and do not want to use DNS, you can configure Unified Communications Manager and IM and Presence Service to use IP addresses rather than hostnames to communicate with gateways and endpoint devices.

You must configure the server to use static IP addressing to ensure that the server obtains a fixed IP address. Using a static IP address also ensures that Cisco Unified IP Phones can register with the application when you plug the phones into the network.

DNS requirements

Note the following requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Unified Communications Manager and IM and Presence Service must either use or not use DNS.

- If your deployment uses DNS—Unified Communications Manager and IM and Presence Service should use the same DNS server. If you use different DNS servers between IM and Presence Service and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS, will need to edit the following Host Name/IP Address fields:
  - Server—In the Cisco Unified CM Administration **Server Configuration** window, set IP addresses for your cluster nodes.
  - IM and Presence UC Service—In the Cisco Unified CM Administration **UC Service Configuration** window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node
  - CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration **CCMCIP Profile Configuration** window, point any CCMCIP profiles to the IP address of the host.
- Multinode considerations—If you are using the multinode feature in IM and Presence Service, see the section regarding multinode deployments in the *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager* for DNS configuration options.

SFTP Server Support

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Solution Partner Program (CSPP). CSPP partners, such as GlobalSCAPE, certify their products with specified versions of Unified Communications Manager. For information on which vendors have certified their products with your version of Unified Communications Manager, go to the following URL and select "Collaboration" from the Technology list in the navigation pane.

https://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supportedUnified Communications Manager versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer tohttp://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Cisco does not support using the SFTP product free FTDP. This is because of the 1GB file size limit on this SFTP product.

For issues with third-party products that have not been certified through the CSPP process, contact the third-party vendor for support.

Platform Requirements

In this release, you cannot install or run Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.

Before you can install or upgrade the software on a virtual machine, you must:

- configure the platform
- install and configure ESXi virtualization software
- deploy the correct OVA template for the release

This section provides information about the platform requirements that you must meet before you can deploy Unified Communications Manager and the IM and Presence Service on virtual machines.

Supported Platforms

Cisco supports virtualized deployments of Unified Communications Manager and the IM and Presence Service on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration.

Whether you use a Cisco Unified Computing System server or a Cisco-approved third-party server configuration, you must ensure that the server meets the configuration requirements of the release. The following options are available:

- a tested reference configuration (TRC)
- a specifications-based configuration

For information about the platform configuration specifications, such as CPU, memory, and storage specifications, see UC Virtualization Supported Hardware.

Information about supported platforms is also available in the following documentation:

- *Cisco Unified Communications Manager on Virtualized Servers*
- *Release Notes* for your product release
- *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager*

Related Topics

Change Virtual Machine Configuration Specifications

ESXi and VMware Tools

You must install a version of vSphere ESXi hypervisor that meets the requirements of the release, as well as VMWare Tools. VMware Tools are specialized drivers for virtual hardware that is installed in the UC applications when they are running virtualized. It is very important that the VMware tools version be in sync with the version of ESXi being used. For more information, see *Cisco Unified Communications Manager on Virtualized Servers*.

If the server is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi.

Related Topics

Upgrade vSphere ESXi
Update VMWare Tools

OVA Templates

Once ESXi is running on the hardware platform, it is ready to host the virtual machines. The first step is to create the virtual machines on the host. You must use Cisco-generated OVA templates to create the virtual machines to run the Unified Communications Manager application. These OVA templates contain aligned

disk partitions and other specific configurations that are required. See Virtualization for Cisco Unified Communications Manager to download the OVA file for your release.

Power Supply

Ensure that you connect each node to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation.

If you want the node to automatically monitor UPS signaling and automatically initiate a graceful shutdown upon power loss, Cisco Unified Communications Manager is dependent on the capabilities of the virtualization software or physical server's service processor. Please see documentation for those products for support, if any.

Software Requirements

The following sections provide information about the software requirements that your deployment must meet.

Browser Requirements

Unified Communications Manager and the IM and Presence Service both provide interfaces that you can use to configure and manage the system. You can access the interfaces by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 1: Supported Browsers and Operating Systems

You can access Unified Communications Manager with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (with latest service pack available)
Mozilla Firefox 3.x or 4.x (if available)	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (latest service pack available) • Apple Mac OS X (latest service pack available)
Safari 4.x or 5.x (if available)	Apple Mac OS X (or newest OS release available)

Upgrade time requirements

The time required to upgrade the software is variable and depends on a number of factors. For large deployments, installation of the upgrade software may take several hours.

Throttling affects time required to upgrade

To preserve system stability during upgrades, the system throttles the upgrade process, which may increase the time required to complete the upgrade.

If the upgrade process is taking much longer than you would like, you can disable throttling. Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance.

To disable throttling, use the following command in the CLI before you start the upgrade:

```
utils iothrottle disable
```

If you want to restart throttling after you start the upgrade, you must cancel the upgrade, restart throttling, and then restart the upgrade.

System availability after upgrade

For standard upgrades, when you activate the upgraded software, the system restarts and is out of service for up to 30 minutes on the publisher node, depending on the size of the database. The length of the outage on subscriber nodes depends on how long database replication takes to complete.

If you need to revert to an earlier software version, you must restart the system which results in a similar service outage period.

Duplicate ENUMS Break Upgrades and Migrations from 9.1(2)

If you are upgrading or migrating from Release 9.1(2) 10.5(2), or 11.0(1) to any later release, an issue exists with older locale installations that causes upgrade and migration failures. This issue exists if any of the following CUCM combined network locales have been installed:

- cm-locale-combined_network-9.1.2.1100-1
- cm-locale-combined_network-10.5.2.2200-1
- cm-locale-combined_network-11.0.1.1000-1

This issue can also occur if the following CUCM locales are installed together in the same cluster:

- cm-locale-en_GB-9.1.2.1100-1
- cm-locale-pt_BR-9.1.2.1100-1
- cm-locale-en_GB-10.5.2.2200-1
- cm-locale-pt_BR-10.5.2.2200-1
- cm-locale-en_GB-11.0.1.1000-1
- cm-locale-pt_BR-11.0.1.1000-1

To ensure that your upgrade does not fail, update your Unified Communications Manager and phone locale installation to use a locale that is dated after August 31, 2017 as this issue does not exist for any locale file issued after that date. After you update your locale installation, you can begin the upgrade or migration. For details on the workaround, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuz97687.

Supported Upgrade Paths

The following sections provide information about the supported upgrade paths for the Cisco Unified Communications Manager and the IM and Presence Service.

Version Requirements

All servers in a cluster must run the same release of Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first three numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2. Refer to the following table for sample Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.

Table 2: Examples of Compatible Unified Communications Manager and IM and Presence Service Versions

Sample Unified Communications Manager Version	Example of Compatible IM and Presence Service Version
10.0.1.30000-2	**10.0.1**.10000-1
10.5.1.10000-7	**10.5.1**.10000-9
10.5.2.10000-5	**10.5.2**.10000-9

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node. For example, if the IM and Presence database publisher node is at version 10.0.1.10000-1, then all IM and Presence subscriber nodes must also be 10.0.1.10000-1.

Release 11.5(1)SU7

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.17900-52
- IM and Presence Service 11.5.1.17900-8

This release offers two main deployment options for the IM and Presence Service:

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU7 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU7 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU7 version.

Release 11.5(1)SU8

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.18900-97
- IM and Presence Service 11.5.1.18900-15

This release offers two main deployment options for the IM and Presence Service:

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU8 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU8 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU8 version.

Upgrade Paths For Cisco Unified Communications Manager

The following tables lists the range of upgrade paths that are supported for the Unified Communications Manager 10.x set of releases, including 10.0(1) and 10.5(1), and 10.5(2). For more detailed information about supported upgrade paths, see the *Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service*.

Refresh upgrades require you to install Cisco Option Package (COP) files. The following table lists the COP files that you need to download for each upgrade path. You must install the required COP files on all nodes before you begin the upgrade process. Ensure that you review the ReadMe file that supports each COP file before you install it.

Upgrade Paths for Release 10.0(x) of Unified Communications Manager

From	To	Upgrade Type
7.x and older:	10.0(x)	Upgrade to 8.6 first, then refresh upgrade to 10.0(x).
8.0(x) to 8.5(x)	10.0(x)	Refresh upgrade Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
8.6(x) to 9.x	10.0(x)	
10.0(1)x	10.0(1)y	Standard upgrade; no COP files required

Upgrade Paths for Release 10.5(x) of Unified Communications Manager

From	To	Upgrade Type
7.x and older	10.5(x)	Upgrade to 8.6 first, then refresh upgrade to 10.5(x).
8.0(x) to 8.5(x)	10.5(x)	Refresh upgrade Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
8.6(x) to 9.x	10.5(x)	
10.x	10.5(x)	Standard upgrade; no COP files required

Upgrade Paths for IM and Presence Service

The following tables list the range of upgrade paths that are supported for the IM and Presence Service 10.x set of releases, including 10.0(1), 10.5(1) and 10.5(2). For more detailed information about supported upgrade paths, see the *Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service*.

Some upgrades require you to install Cisco Option Package (COP) files. The following table lists the COP files that you need to download for each upgrade path. You must install the required COP files on all nodes before you begin the upgrade process. Ensure that you review the ReadMe file that supports each COP file before you install it.

Upgrade Paths for Release 10.0(x) of IM and Presence Service

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(3) and earlier	10.0(x)	Upgrade to 8.6(5)su5 first, then refresh upgrade to 10.0(x)
8.5(4)	10.0(x)	Refresh upgrade Required COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn
8.6(3) to 9.x	10.0(x)	Refresh upgrade Required COP file: • ciscocm.version3-keys.cop.sgn

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
10.0.1.x	10.0(x)	Standard upgrade; no COP file required

If you are upgrading from IM and Presence Service 10.0(1) Export Unrestricted to any higher release of IM and Presence Service Export Unrestricted (including Service Updates), you must install the following COP file before you begin the upgrade: `ciscocm.cup.unrst_upgrade_10_0_1_v1.2.cop.sgn`. You can download this file from Cisco.com.

Upgrade Paths for Release 10.5(x) of IM and Presence Service

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(3) and earlier	10.5(x)	Upgrade to 8.6(5)su5 first, then refresh upgrade to 10.5(x).
8.5(4)	10.5(x)	Refresh upgrade Required COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn
8.6(3) to 9.x	10.5(x)	Refresh upgrade Required COP file: • ciscocm.version3-keys.cop.sgn
10.x	10.5(x)	Standard upgrade; no COP file required

Upgrade From Cisco Unified Presence Release 8.5(4)

If you upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5 to the current release, note the following:

- If you have intercluster peers to Cisco Unified Presence Release 8.0(x) or Release 8.5 clusters, you will not have intercluster availability until you upgrade all of these clusters to Release 8.6 or to Release 9.x and later. After the upgrade is complete, the previously configured peers will start working and intercluster availability will be restored.
- If you upgrade a Cisco Unified Presence Release 8.5 cluster that has High Availability (HA) enabled to Release 9.x or later, Cisco recommends that you disable HA on each presence redundancy group before you begin the upgrade. You can reenable HA on each cluster after the switch version is complete, database replication is complete, and all services are back up and running.
- During a software upgrade, the Cisco Replication Watcher service delays feature service startup on the publisher node for up to 20 minutes and on subscriber nodes indefinitely until replication is established.

Note As of IM and Presence Release 10.0(1), the Cisco Replication Watcher service has been renamed to the Cisco IM and Presence Data Monitor service.

Licensing Requirements

The following sections provide information about the licensing requirements for Unified Communications Manager and the IM and Presence Service

Cisco Unified Communications Manager License Requirements

Use the Cisco Prime License Manager to allocate and monitor the licenses for Unified Communications Manager, its applications, and endpoints. See the *Cisco Prime License Manager User Guide* for information about generating and installing licenses.

Important Unused PAKs and/or licenses for versions prior to Release 9.0 cannot be installed once your system has been upgraded to Release 9.0 or later. If you have uninstalled PAKs, install all licenses before upgrading.

IM and Presence license requirements

The IM and Presence Service Service does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service Service for each assigned user.

Note With the Jabber for Everyone offer, no end user licenses are required to enable IM and Presence functionality. For more information, see *"Jabber for Everyone Quick Start Guide"*.

You can assign IM and Presence Service on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence Service to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for IM and Presence Service, they will not be able to log in to the IM and Presence Service server to view the availability of other users, send or receive IMs, and other users will not see their availability status.

You can enable a user for IM and Presence Service using any of the following options:

- The **End User Configuration** window in Unified Communications Manager. For more information, see Administration Guide for Cisco Unified Communications Manager.
- The Bulk Administration Tool (BAT)
- Assign IM and Presence Service to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

For more information, see the IM and Presence Service chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

IM and Presence Service capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence Service capabilities can also be acquired for users that are not Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. For more information, see *Jabber for Everyone Quick Start Guide*.

Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and IM and Presence Service 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 IM and Presence Service 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 ofUnified Communications Manager and IM and Presence Service.

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.

GUI Item	Location	Description
Cisco Unified CM IM and Presence Administration		
Security Settings	**System** > **Security** > **Settings**	• 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**	• 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.
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.