Installation Planning

The following sections provide information about the installation requirements.

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 Cisco Unified Communications Manager or IM and Presence Service.

⚠

Caution Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco 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 and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Limitations

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

Subnet Limitations

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

Cluster Size

The number of Cisco 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 Cisco Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

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

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

Network Requirements

This section lists the requirements that your network must meet before you can deploy Cisco 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 Cisco 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 Cisco Unified Communications Manager (Unified Communications Manager) and IM and Presence must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence should use the same DNS server. If you use different DNS servers between IM and Presence 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, see the section regarding multinode deployments in the *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager* for DNS configuration options.

Firewall Requirements

Make sure that you configure your firewall so that connections to port 22 are open, and are not throttled. During the installation of IM and Presence subscriber nodes, multiple connections to the Cisco Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation.

Platform Requirements

In this release, 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.

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 Cisco Unified Communications Manager and the IM and Presence Service on virtual machines.

Software Requirements

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

Version Requirements

All servers in a cluster must run the same release of Cisco 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 Cisco Unified Communications Manager software version 10.0.1.30000-2. Refer to the following table for sample Cisco Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.

Table 1: Examples of Compatible Cisco 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.

Software Restrictions

You cannot install or use third-party or Windows-based software applications. The system can upload and process only software that Cisco Systems approves. You must perform all software installations and upgrades using Cisco Unified Communications Operating System Administration.

For information about software compatibility for IM and Presence nodes, see the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*.

For information about software compatibility for Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Browser Requirements

Cisco 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 2: Supported Browsers and Operating Systems

You can access Cisco 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)

User Name and Password Requirements

The following sections provide information about the account names and passwords that you must configure for Cisco Unified Communications Manager and the IM and Presence Service.

Accounts and Passwords for Unified Communications Manager

User Name and Password Requirements

Note The system checks your passwords for strength. See topics related to password considerations for guidelines on creating a strong password.

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password
- Application User name and password
- Security password

Administrator Account User Name and Password

You use the Administrator Account user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Application User Name and Password

When you install Cisco Unified Communications Manager, you must enter an Application User name and password. You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Real Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User name - The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password - The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

Caution Do not use the system application name as the Application User name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database.

System application names are:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

You can change the Application User name and password by using the command line interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Security Password

During the installation, you must specify a security password. Cisco Unified Communications Manager systems use this password to authorize communications between nodes in the cluster, including IM and Presence Service nodes. The security password must be identical on all nodes in the cluster.

The Security password must be minimum six characters long and can contain alphanumeric characters, hyphens, and underscores.

If you are enabling FIPS, Common Criteria, or Enhanced Security mode on the cluster, ensure that the security password is minimum 14 characters.

If your security password is less than 14 characters:

- Upgrades from any previous versions of FIPS enabled Cisco Unified Communications Manager to Release 12.5 or later aborts with an error message.
- You must set the security password to a minimum of 14 characters to resume the upgrade process.

Accounts and Passwords for IM and Presence Service

Required passwords

During installation of the IM and Presence Service, you must specify the following usernames and passwords:

Administrator account username and password

During installation, you must create an Administrator Account username and password to log into the following areas:

- Cisco Unified Operating System Administration interface
- Disaster Recovery System Administration interface
- Command Line Interface (CLI)

The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

If you lose the Administrator password and cannot access the system, you can recover the Administrator password in Cisco Unified Communications Operating System Administration.

If you need to reset the Administrator password, use the CLI.

Application username and password

During the installation of Cisco Unified Communications Manager, you are prompted to create an Application User name and password. Use this same Application User name and password when you sign into the Cisco Unified CM IM and Presence Administration interface.

If you need to reset the Application User password, use the CLI.

InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated

The application user group roles InterCluster Peer-User and Admin-CUMA are deprecated from release 10.0(1). Any application users with these roles configured in releases 8.x or 9.x have the roles removed during an upgrade to any 10.x release. After the upgrade the administrator must configure appropriate roles for these users.

Note For intercluster to function correctly, the AXL user defined on the IM and Presence Service user interface (**Presence** > **Inter-Clustering**) must have a Standard AXL API Access role associated with it on the Cisco Unified Communications Manager application user page.

Password Recommendations

The installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include special symbols.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, such as aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.

- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

Installation Time Requirements

Time Requirements for Cisco Unified Communications Manager

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes, depending on your server type.

Time Requirements for IM and Presence Nodes

The entire IM and Presence installation process, excluding pre- and post-installation tasks, takes approximately 45 to 90 minutes per server, depending on your server type.

Licensing

The following sections provide information about the licensing requirements for Cisco 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 Cisco 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 does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service for each assigned user.

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

You can assign IM and Presence on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence to a user, this enables the user to send and receive IMs and also to send and receive availability updates. If users are not enabled for IM and Presence, they will not be able to log in to the IM and Presence 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 using any of the following options:

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

See the IM and Presence chapter in the *Cisco Unified Communications Manager Features and Services Guide* for more information.

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

Required Installation Information

When you install either Cisco Unified Communications Manager or the IM and Presence Service on a server, the installation process requires you to provide specific information. You can provide this information manually during the installation process or you can provide it using an answer file. For each server that you install in a cluster, you must gather this information before you begin the installation process.

The following table lists the information that you must gather before you begin the installation.

Note Because some of the fields are optional, they may not apply to your configuration. For example, if you decide not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

You cannot change some of the fields after the installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a parameter after installation, and if you can, it provides the appropriate menu path or Command Line Interface (CLI) command.

Cisco recommends that you make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

Table 3: Required Installation Information

Configuration data	Description	Editable after installation
Administrator Credentials		
Administrator Login	Specifies the name that you want to assign to the Administrator account.	No After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password	Specifies the password for the Administrator account.	Yes CLI: `set password user admin`

Configuration data	Description	Editable after installation
Application User Credentials		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: `utils reset_application_ui_administrator_name`
Application User Password	Specifies the password for applications on the system.	Yes CLI: `utils reset_application_ui_administrator_password`
Security Password		
Security password for Cisco Unified Communications Manager	Servers in the cluster use the security password to communicate with one another. Set this password on the Cisco Unified Communications Manager publisher node, and enter it when you install each additional node in the cluster, including IM and Presence nodes.	Yes. You can change the security password on all nodes in the cluster using the following CLI command: `set password user security`
Certificate Information		
Organization	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state] [country]`
Unit	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state] [country]`
Location	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state] [country]`
State	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state] [country]`

Configuration data	Description	Editable after installation
Country	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state]`
(Optional) SMTP		
SMTP Location	Specifies the name of the SMTP host that is used for outbound email. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.	Yes • In Cisco Unified Communications Operating System Administration: select **Settings** > **SMTP** and enter the IP address or Hostname in the SMTP Host Field. • CLI: `set smtp [host]`
NIC Interface Settings		
NIC Speed	If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) speed, you must select the NIC speed (either 10 megabit or 100 megabit).	Yes CLI: `set network nic eth0 {auto | {en| dis}} {speed| {10| 100}} {duplex half| {half| full}}` **Note** 1000BASE-T can only be enabled via auto-negotiation. **Note** Virtual machines do not support this command.
NIC Duplex	If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) duplex setting, you must select the NIC duplex setting (either Full or Half).	Yes CLI: `set network nic eth0 {auto | {en| dis}} {speed| {10| 100}} {duplex half| {half| full}}` **Note** 1000BASE-T can only be enabled via auto-negotiation. **Note** Virtual machines do not support this command.

Configuration data	Description	Editable after installation
MTU Size **Note** The MTU setting must be the same on all nodes in a cluster.	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. The value must not exceed the lowest MTU size that is configured on any link in your network. Default: 1500 bytes	Yes CLI: `set network mtu [size]`
Network Information		
DHCP (Dynamic Host Configuration Protocol)	Select **Yes** if you want to use DHCP to automatically configure the network settings on your server. If you select **No**, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration.	Yes. • In Cisco Unified Operating System Administration: select **Settings** > **IP** > **Ethernet** • CLI: `set network dhcp eth0 [enable]` CLI: `set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]`
Hostname	If DHCP is set to No, you must enter a hostname for this machine.	Yes; for Cisco Unified Communications Manager nodes, choose one of the following: • In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet** • CLI: `set network hostname` You will be prompted to enter the parameters. To change the hostname on a IM and Presence server, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*.

Configuration data	Description	Editable after installation
IP Address	If DHCP is set to No, you must enter the IP address of this machine.	Yes; for Cisco Unified Communications Manager nodes, choose one of the following: • In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet** • CLI: `set network IP eth0 [ip-address] [ip-mask]` To change the IP address on a IM and Presence server, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*.
IP Mask	If DHCP is set to No, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. The subnet mask must use the following format: 255.255.255.0	Yes • In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet** • CLI: `set network IP eth0 [ip-address] [ip-mask]`
Gateway Address	If DHCP is set to No, you must enter the gateway address.	Yes. • In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet** • CLI: `set network gateway [addr]`
(Optional) DNS		
DNS Primary	If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames.	Yes CLI: `set network dns primary [address]`
DNS Secondary	When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server.	Yes CLI: `set network dns secondary [address]`
Domain	Represents the name of the domain in which this machine is located	Yes CLI: `set network domain [name]`

Configuration data	Description	Editable after installation
Timezone		
Time Zone	Reflects the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your machine.	Yes CLI: **`set timezone [zone`**
Network Time Protocol		
NTP Server IP Address	During installation of the IM and Presence publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. Cisco recommends that you use the Cisco Unified Communications Manager publisher node as the NTP server.	Yes In Cisco Unified Communications Operating System Administration, select **Settings** > **NTP Servers**

Export Restricted and Export Unrestricted Software

This release of Cisco 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, Cisco Unified Communications Manager and IM and Presence nodes 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 IM 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**	• 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** has been removed.
Service Parameter Confiugration 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 has 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.