Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)

First Published: 2019-01-23

Last Modified: 2021-10-04

CONTENTS

CHAPTER 1

Planning the Installation

Installation Methods

This guide covers the following installation methods for Cisco Unified Communications Manager and the IM and Presence Service:

Installation Method	Description
Basic Install of Cluster	This method contains the typical installation of a Cisco Unified Communications Manager and IM and Presence Service cluster. In this method, you must install the publisher node first, and then add and install your subscriber nodes. Basic Installation includes the following custom cases: • Apply a Patch During an Upgrade—If a newer version exists than the image that you are installing, you can apply a patch to your install image and upgrade to the newer version. This option is available for Unified Communications Manager only. • Pre-installed Software—If you have a new server with either Unified Communications Manager or IM and Presence Service software pre-installed (for example, Cisco Business Edition) you can configure the pre-installed software.
Touchless Install of Cluster	Touchless installation allows you to complete a full cluster installation for Unified Communications Manager and IM and Presence Service in one seamless process. Once you provide the server details for all cluster nodes and start the installation, the system installs software on all cluster nodes dynamically, without manual intervention from the administrator. This method is particularly useful if you have a large cluster to install.

Installation Method	Description
Add a Node to a Cluster	Use these procedures to add and install a new node in an existing cluster. The new node(s) must be added as a subscriber node.

Note You can also use Cisco Prime Collaboration Deployment to install your cluster. For more information, see *Cisco Prime Collaboration Deployment Administration Guide*.

Topology Options

This section provides an overview of the system topology and describes the relationship between the types of nodes in the topology.

Clusters

Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features and enable system scalability.

A cluster comprises a set of Unified Communications Manager nodes and IM and Presence nodes that run compatible software versions.

Publisher Nodes and Subscriber Nodes

Within a cluster, there is a database publisher for each type of node that you install.

When you install Unified Communications Manager, the installation wizard prompts you to specify whether the node you are installing is the first node in the cluster. The first Unified Communications Manager node that you install becomes the publisher node, because it publishes the voice and video database to the other Unified Communications Manager nodes in the cluster. All subsequent nodes in the cluster are called subscriber nodes. Each subscriber node must be associated with the publisher node. You must set up all subscriber nodes in the system topology on the publisher node before you install the software on the subscriber nodes.

When you install IM and Presence nodes, the first node that you install functions as the server for the IM and Presence database. Because this node publishes the database for all of the IM and Presence nodes in the cluster, it is referred to as the IM and Presence database publisher; however, you must install this and all other IM and Presence nodes as subscribers of the Unified Communications Manager publisher node. As with other subscriber nodes, you must add these in the system topology before you install the software.

Topology Options

When installing your cluster, you must decide on the topology that you want to deploy. For example:

- The number of cluster nodes required.

- Whether you will install all cluster nodes in a single location, or if you will install your nodes in separate geographic sites connected via a WAN in order to provide geographic redundancy.

- For IM and Presence deployments, install a standard deployment or an IM and Presence Central Cluster deployment.

For information on planning a Cisco Collaboration deployment, and choosing your topology for more information, see to the *Cisco Collaboration System Solution Reference Network Desig*n at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Cluster Topology for IM and Presence

If you are deploying the IM and Presence Service, you must decide before you begin the installation whether you want a Standard Deployment (IM and Presence Service on Unified Communications Manager) or an IM and Presence Central Cluster deployment. Refer to the following table for a description of each option.

IM and Presence Deployment	Description
Standard Deployment (Decentralized)	The IM and Presence cluster is installed on the same servers as the Unified Communications Manager telephony cluster. The IM and Presence cluster shares a platform and many of the same services as the telephony cluster. This option requires a 1x1 mapping of telephony clusters to IM and Presence clusters. Basic installations follow this process: 1. Install the Unified Communications Manager publisher node 2. Install the Unified Communications Manager subscriber nodes 3. Install the IM and Presence Service publisher node 4. Install the IM and Presence Service subscriber nodes For touchless installations, you can install all Unified Communications Manager and IM and Presence Service cluster nodes in a single process.
Centralized Deployment	The IM and Presence Service central cluster is installed separately from your telephony cluster and may be located on completely different hardware servers. This deployment removes the 1x1 mapping requirement between telephony clusters and IM and Presence clusters. This allows you to scale your telephony deployment and IM and Presence deployment separately. For basic installations: 1. Install a local Unified Communications Manager publisher node in the central cluster. This node is not a part of your telephony deployment. The node handles functions like database and user provisioning for the central cluster. 2. Install the IM and Presence Service database publisher node. 3. Install any IM and Presence subscriber nodes. For touchless installations, you can install your local Unified Communications Manager publisher node and your IM and Presence Service central cluster in a single process. However, your telephony cluster must be installed separately.

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.

Note If you upgrade Unified Communications Manager which has IPsec configured using a certificate-based authentication with self-signed certificate, then the upgrade fails. To perform a successful upgrade, you have to reconfigure the IPsec policy with a CA-signed certificate.

Note
  - By default, your system is in non-FIPS mode, you must enable it.

  - Ensure that the security password length is minimum 14 characters before you upgrade to FIPS, Common Criteria, or Enhanced Security mode on the cluster. Update the password even if the prior version was FIPS enabled.

Note Unified Communications Manager 12.5 requires minimum ESXi version of 6.5 U2 with minimum VM Hardware version of 13. For more information on latest Unified Communications Manager ESXi version support, see http://www.cisco.com/go/virtualized-collaboration.

Note The Simplified Upgrade (Cluster upgrade, reboot, and switch version) feature is supported only in Unified Communications Manager version 12.5 and higher.

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

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.

Firewall Requirements

Ensure 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 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 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

> **Note** Unified Communications Manager 12.5 requires minimum ESXi version of 6.5 U2 with minimum VM Hardware version of 13. For latest Unified Communications Manager ESXi version support, see http://www.cisco.com/go/virtualized-collaboration.

- 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 Versions

The following software versions apply to Release 12.5(1):

- Unified Communications Manager 12.5.1.10000-22

- IM and Presence Service Service 12.5.1.10000-22

Version Mismatches

This release offers two main deployment options for this release of Unified Communications Manager and the IM and Presence Service Service:

- Standard Deployments—Both Unified Communications Manager and the IM and Presence Service Service must be running the above 12.5.1.10000-22 version for your deployment to be supported. A version mismatch is not supported.

- Centralized Deployments of IM and Presence Service Service—If you have the Centralized Deployment option configured on theIM and Presence Service Service, then within the IM and Presence Service central cluster, both the Unified Communications Manager instance and the IM and Presence Service Service must be running a 12.5.1.10000-22 version. However, the telephony cluster that the central cluster connects to does not have to be running a 12.5.1.10000-22 version.

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 Unified Communications Manager, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Username and Password Requirements

During the installation, you must specify the following usernames and passwords:

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

Administrator Account

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

When you install 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 username - The Application User username 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. Unified Communications Manager systems use this password to authorize communications between nodes in the cluster, including IM and Presence Service nodes. This password must be identical on all nodes in the cluster.

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

Password Recommendations

The installation wizard ensures 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 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 Requirements

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

Note   As of Unified Communications Manager Release 12.0(1), Smart Licensing replaces Prime License Manager. Smart Licensing requires you to have a Smart Account created and configured before you upgrade or migrate the Unified Communications Manager server.

Several deployment options through which Unified Communications Manager can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite are:

- Direct—Unified Communications Manager sends usage information directly over the internet. No additional components are needed.

- Cisco Smart Software Manager satellite—Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

Note	Cisco Smart Software Manager satellite is an on-premises collector similar to standalone Prime License Manager.

- Proxy Server—Unified Communications Manager sends usage information over the internet through a proxy server.

Cisco Unified Communications Manager License Requirements

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Cisco Smart Software Manager replaces Prime License Manager in Unified Communications Manager Release 12.0(1) and later versions. Cisco Prime License Manager is no longer used as of Release 12.0(1) and no longer appears in the Installed Applications pre-login screen.

If you have enabled the mixed-mode prior to upgrade and have not registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite then,

- You see the warning message in the Cisco Unified CM Administration page and Cisco Unified OS Administration page as stated below:

Warning	The system is currently running Mixed mode. To continue running Mixed mode, please ensure Smart Licensing registration is completed using the Registration Token received from the Smart/Virtual Account that has Allow export-controlled functionality checked.

- An alert named *SmartLicenseExportControlNotAllowed* is sent, when the Unified Communications Manager is not registered with the Registration Token.

For details on how to configure Cisco Smart Software Licensing, see "Smart Software Licensing" chapter, located within the "Configure Initial Parameters for the System" at System Configuration Guide for Cisco Unified Communications Manager.

For more details on Cisco Smart Software Manager satellite, including the *Smart Software Manager satellite Installation Guide*, see http://www.cisco.com/go/smartsatellite.

Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate

this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.

Unified Communications Manager 9.0x and later version of 12.0(1)

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.

- Two types of Migration are supported:

    - PAK based—Supported for already fulfilled, partially fulfilled and unfilled PAKs

    - Device based

- Partial Conversion supports mixed environment of older and Unified Communications Manager 12.0(1) clusters.

Upgrade to Smart Entitlement

Unified Communications Manager Pre 9.0x (Device based) to 12.0(1)

You may contact Cisco Global Licensing Operations (GLO) for helping with migrating Device-based licenses to Smart Entitlement.

Customer may establish equivalent user-based licensing required by running License Count Utility (LCU). For more details, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/uct/CUCM_BK_ UCT_Admin_Guide/CUCM_BK_UCT_Admin_Guide_chapter_01.html.

From the LCU report, Customer may order respective quantity of Upgrade Licenses through Cisco Commerce Workspace. Beyond this, they would have to buy additional new licenses. For more details, see the Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.

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 System Configuration Guide for Cisco Unified Communications Manager.

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*.

Required Installation Information

When you install either 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.

We recommend 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 1: 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`
Application User Credentials		

Configuration data	Description	Editable after installation
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 Unified Communications Manager	Servers in the cluster use the security password to communicate with one another. Set this password on the 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 command: CLI: `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]`
Country	Used to create the Certificate Signing Request.	Yes CLI: `set web-security [orgunit] [orgname] [locality] [state]`

Configuration data	Description	Editable after installation
(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.
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		

Configuration data	Description	Editable after installation
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 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*.
IP Address	If DHCP is set to No, you must enter the IP address of this machine.	Yes; for 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*.

Configuration data	Description	Editable after installation
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]`
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		

Configuration data	Description	Editable after installation
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 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 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.
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**.

GUI Item	Location	Description
Proxy Configuration Settings	**Presence** > **Routing** > **Settings**	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.

Preinstallation Tasks

- Preinstall Tasks for Cisco Unified Communications Manager, on page 21
- Preinstall Tasks for the IM and Presence Service, on page 23
- Enable the Cisco AXL Web Service, on page 25
- Verify DNS Registration, on page 25

Preinstall Tasks for Cisco Unified Communications Manager

Procedure

	Command or Action	**Purpose**
Step 1	Planning the Installation, on page 1	Review the Planning chapter. Make sure to review the following: • Decide on your installation method. • Decide on your cluster topology. • For IM and Presence, decide whether you are installing a standard deployment or an IM and Presence central cluster. • Review the Requirements and Limitations,
Step 2	Required Installation Information, on page 12	Review the installation requirements and record the configurations settings for each server that you plan to install.
Step 3	Create virtual machines.	• Get base OVA. • Run Collab Sizing Tool to get the required virtual machine count and specs of each virtual machine. If you don't want to run Collab Sizing Tool, follow the guidance in the OVA readme and the OVA wizard to pick a predefined starting

	Command or Action	Purpose
		point, which can be changed later if needed. • If you are installing from a skip-install OVA from the factory preload of a Business Edition appliance, see *Installation Guide for Cisco Business Edition 6000* or *Installation Guide for Cisco Business Edition 7000*.
Step 4	Mount the installation ISO file.	Place the installation ISO file in a location where the virtual machine can access it and edit the virtual machine's DVD drive to map to the file. Select the option to mount the DVD drive when you power on the virtual machine. When you power on the virtual machine, it will mount the ISO file and start the installation process. Do not begin the installation process until you have completed all of the steps in this procedure.
Step 5	Verify that the links between servers meet the 80-ms round-trip time (RTT) requirement and that you have enough bandwidth to support database replication.	For more information on the 80-ms RTT requirement, see the *Cisco Unified Communications Solutions Reference Network Design* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html
Step 6	Verify the NTP status on the publisher node.	If the publisher node fails to synchronize with an NTP server, subscriber node installation can fail. On the Cisco Unified Communications Manager publisher node, run the `utils ntp status` CLI command.
Step 7	Complete the following firewall updates: • If a firewall is in the routing path between nodes, disable the firewall. • Increase the firewall timeout settings until after you complete the installation.	Temporarily allowing network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to IP any/any) does not always suffice. The firewall might still close necessary network sessions between nodes due to timeouts.
Step 8	Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between servers where you are installing Unified Communications Manager.	
Step 9	Verify the NIC speed and duplex settings.	Ensure that the network interface card (NIC) speed and duplex settings on the switch port are the same as those that you plan to set on the new server.

	Command or Action	Purpose
		For GigE (1000/FULL), you should set NIC and switch port settings to `Auto/Auto`; do not set hard values.
Step 10	Enable PortFast on all switch ports that are connected to Cisco servers.	With Portfast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay [the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].
Step 11	If you use DNS, verify that all servers on which you plan to install Unified Communications Manager are properly registered in DNS.	For details, see Verify DNS Registration, on page 25
Step 12	If you are using a server that is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, disable the SATA controller in the BIOS.	The ICH10 onboard SATA controller is not supported by EX/. Do the following: a. Boot the server and press **F2** when prompted during bootup. b. Select the **Advanced** tab. c. Select the **Mass Storage Controllers Configuration**. d. Set the **Onboard SATA Controller** to **Disabled**.
Step 13	Licensing Requirements, on page 9	Make sure that your system has adequate licensing.

Preinstall Tasks for the IM and Presence Service

Procedure

	Command or Action	Purpose
Step 1	Planning the Installation, on page 1	Review the Planning chapter. Make sure to review the following: • Decide on your installation method and cluster topology. • For IM and Presence, decide whether you are installing a standard deployment or an IM and Presence central cluster. • Review the Requirements and Limitations.

	Command or Action	Purpose
Step 2	Supported Version	Make sure that the Unified Communications Manager and IM and Presence Service software versions are compatible.
Step 3	Required Installation Information, on page 12	Gather all the information you need to complete the installation and configuration of the IM and Presence.
Step 4	Create your virtual machines.	For every node in your cluster, create virtual machines using the Virtual Server Template (OVA file) that is recommended for your release.
		Different OVA files are available; choose the correct OVA file based on the environment in which you are deploying Unified Communications Manager. For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html.
Step 5	Verify network connectivity.	Make sure that each IM and Presence server has network access to the Unified Communications Manager publisher server. Ping the Cisco Unified Communications Manager publisher node from the other IM and Presence servers.
Step 6	Enable the Cisco AXL Web Service, on page 25	Make sure that the Cisco AXL Web Service is enabled.
Step 7	Verify DNS Registration, on page 25	If you use DNS, ensure that you have configured the hostname of the new IM and Presence server on the DNS server and that the DNS server can resolve the hostname of the Unified Communications Manager publisher server and of other IM and Presence servers (if any).
		Note We recommend that you use the same DNS servers between IM and Presence and Unified Communications Manager. If you use different DNS servers, it is likely to cause abnormal system behavior. Both Unified Communications Manager and IM and Presence must either use DNS, or not use DNS, because it does not support mixed-mode deployments.

Enable the Cisco AXL Web Service

Verify that the Cisco AXL Web Service is running.

Procedure

Step 1   Log in to the Cisco Unified Serviceability interface.

Step 2   Choose **Tools** > **Service Activation**.

Step 3   Under **Database and Admin Services**, make sure that the **Cisco AXL Web Service** status indicates **Activated**.

Step 4   If the status says **Deactivated**, activate it by checking the adjacent check box and clicking **Save**.

Verify DNS Registration

Follow this procedure if you use a DNS in your topology. You must verify that all servers to be added are registered in DNS properly by performing the following actions:

Procedure

Step 1   Open a command prompt.

Step 2   To ping each server by its DNS name, enter ping DNS_name.

Step 3   To look up each server by IP address, enter nslookup IP_address.

CHAPTER 3

Installation Tasks

Installation Task Flows

Choose one of the following installation task flows:

Task Flow	Description
Cluster Installs	
Basic Installation Task Flow, on page 29	Use this method for basic installs of any of the following deployments: • Cisco Unified Communications Manager telephony cluster installs • Standard Deployments (Decentralized) for IM and Presence
Install IM and Presence Central Cluster (Basic Installation), on page 31	For Centralized Deployments of IM and Presence, use this task flow for basic installs of the IM and Presence central cluster.
Touchless Installation Task Flow, on page 44	Use this task flow to install a Unified Communications Manager or IM and Presence Service cluster dynamically without the need for manual intervention. Applies to either Centralized or Standard (Decentralized) IM and Presence deployments.
Node Installs	
Add a New Node to an Existing Cluster, on page 49	Complete these tasks if you want to add a node to an existing Unified Communications Manager or IM and Presence Service cluster.

> **Note** You can also use Cisco Prime Collaboration Deployment to install your cluster. For motr information, see *Cisco Prime Collaboration Deployment Administration Guide*.

Before You Begin

Before you begin the installation, review the following information:

- Make sure that the subscriber nodes that you are installing can connect to the publisher node server during the installation.

- Make sure that all Unified Communications Manager servers in a cluster have the same software version. Make sure that all IM and Presence servers in a cluster have the same version of the released software. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed. If you are installing IM and Presence nodes, Unified Communications Manager and IM and Presence Service software versions must have the same major and minor release number.

- If you are installing on an existing cluster, do not attempt to perform any configuration tasks during the installation.

- Be aware that directory names and filenames that you enter while you are running the installation program are case-sensitive.

- For IM and Presence Service installations, make sure that you know whether you are installing IM and Presence Service in a Centralized Deployment or in a Standard Deployment (Decentralized). For details, see Cluster Topology for IM and Presence, on page 3.

Installation Wizard

The following table provides instructions on how to navigate within the installation wizard.

Table 2: Installation Wizard Navigation

To Do This	Press This
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Space bar or Enter
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or Enter to choose Back (when available)
Get help information on a window	Space bar or Enter to choose Help (when available)

Note   The installation wizard supports the following characters:

- alphanumeric: A-Z, a-z, and 0-9- spaces

- spaces and # (except as the first character)

- only the following special characters: \.,-_:;{}()[]

all other characters are not supported.

Basic Installation Task Flow

Complete the following tasks to install Unified Communications Manager and IM and Presence Service cluster using the basic installation process:

- Installs of a Cisco Unified Communications Manager telephony cluster

- Installs of the IM and Presence Service in a Standard Deployment (Decentralized).

Note   Depending on your installation scenario, you may not need to perform all of the tasks. For example, if you are installing the IM and Presence Service on an existing Unified Communications Manager cluster that is already in use, you only need to complete the tasks for installing the IM and Presence Service.

Before You Begin

	Cisco Unified Communications Manager	IM and Presence Service	Description
Step 1	Basic Installation, on page 32	—	Begin the install process for Unified Communications Manager.
Step 2	Enter Configuration Information for Preinstalled Servers, on page 33	—	Pre-installed servers only (e.g., Cisco Business Edition). Add pre-configured information to the installation. Otherwise, skip this task.

	Cisco Unified Communications Manager	**IM and Presence Service**	**Description**
Step 3	Optional. Complete either of the following tasks: • Upgrade Install Image from Local Source, on page 34 • Upgrade Install Image from Remote Server, on page 35	—	Upgrade your install image to a newer version. This optional task is available for Unified Communications Manager installs only.
Step 4	Configure Basic Installation, on page 37	—	Continue with the Basic Installation process by configuring your installation.
Step 5	Configure the Unified Communications Manager Publisher, on page 39	—	Configure and install software on the publisher node.
Step 6	Add Subscriber Nodes, on page 42	—	Add subscriber nodes to the publisher node.
Step 7	Install Subscriber Nodes, on page 43	—	Install software on your Cisco Unified Communications Manager subscriber nodes.
Step 8	—	Basic Installation, on page 32	Begin the install process for the IM and Presence Service.
Step 9	—	Enter Configuration Information for Preinstalled Servers, on page 33	Pre-installed servers only (e.g., Cisco Business Edition). Add pre-configured information to the installation. Otherwise, skip this task.
Step 10	—	Configure Basic Installation, on page 37	Continue Basic Install process for IM and Presence by configuring the installation.
Step 11	—	Configure the IM and Presence Publisher, on page 42	Configure and complete the installation for the IM and Presence database publisher node.
Step 12	Add Subscriber Nodes, on page 42	—	On the Cisco Unified Communications Manager publisher node, add IM and Presence subscribers.

	Cisco Unified Communications Manager	IM and Presence Service	Description
Step 13	—	Install Subscriber Nodes, on page 43	Install software on your IM and Presence Service subscriber nodes.

Install IM and Presence Central Cluster (Basic Installation)

Complete these tasks to install an IM and Presence Service Centralized Deployment using Basic Installation.

- Unified CM Publisher (non-telephony)—The IM and Presence central cluster requires a local Unified Communications Manager publisher node within the central cluster for database and user provisioning. This node does not handle telephony. There is no need to install subscriber nodes.

- IM and Presence Central Cluster

Note
For basic installation of IM and Presence Service in a Decentralized (Standard) deployment, follow the to install both the telephony and IM and Presence clusters.

	Unified CM Publisher (non-telephony)	IM and Presence Central Cluster	Description
Step 1	Basic Installation, on page 32		Begin the install process for the Unified CM publisher node.
Step 2	Configure Basic Installation, on page 37		Configure the Basic Installation.
Step 3	Configure the Unified Communications Manager Publisher, on page 39		Configure the Unified CM publisher node.
Step 4		Basic Installation, on page 32	Begin the install process for the IM and Presence central cluster.
Step 5		Configure Basic Installation, on page 37	Continue with the Basic Install process for IM and Presence by continuing the installation.
Step 6		Configure the IM and Presence Publisher, on page 42	Configure the IM and Presence database publisher node.
Step 7	Add Subscriber Nodes, on page 42		On the Unified CM publisher, add IM and Presence subsciber nodes.
Step 8		Install Subscriber Nodes, on page 43	Complete the installation on the IM and Presence subsicribers.

Basic Installation

Use this procedure for Unified Communications Manager and IM and Presence Service installations to begin the basic install process. You can use this procedure if you are installing a cluster or adding a node to an existing cluster.

Procedure

___

Step 1   If you are using a configuration file created by the Answer File Generator, ensure that virtual floppy image in a location where the virtual machine can access it.

Note   If you have a Cisco Business Edition 6000/7000 appliance with the software pre-installed, you do not need to install from a DVD or ISO file, unless you want to re-image the server with a later product release. Go directly to the configure basic installation procedure to enter the configuration information. For more information, see *Installation Guide for Cisco Business Edition 6000* or *Installation Guide for Cisco Business Edition 7000*.

Step 2   Perform one of the following:

   • If you are installing from a DVD drive a VMware ESXi server host, insert the installation DVD into the tray and restart the virtual machine, so that it boots from the DVD.
   • If you are installing from a data store ISO file located on the local ESXi host or on a storage area network (SAN), edit the CD or DVD drive on the virtual machine to select the data store ISO file. Select the option to connect at power on, and restart the virtual machine. If you have configured the virtual machine to use the ISO at the same time that you created the virtual machine using the OVA file, skip this step and complete the rest of the procedure.

After the server completes the boot sequence, the **DVD Found** window displays.

Step 3   Click **Yes** to perform the media check. Or click **No** to skip the media check.

The media check verifies the integrity of the DVD. If the DVD has passed the media check previously, choose to skip the media check.

Step 4   If you click **Yes** to perform the media check, the **Media Check Result** window displays.

   a) If the **Media Check Result** displays **Pass**, click **OK** to continue the installation.
   b) If the media check fails, either download another copy from cisco.com or obtain another DVD directly from Cisco.

Step 5   In the **Product Deployment Selection** window, specify which product you want to install:

   • Unified Communications Manager—Choose the product and click **OK**.
   • IM and Presence Service—Select **OK**.
   • Cisco Unity Connection—Select the product and click **OK**.

Note   The window displays the products that are supported and not supported by your hardware. If only one product is supported, you do not choose which product to install.

Step 6   If the software is currently installed on the server, the **Overwrite Hard Drive** window opens and displays the current software version on your hard drive, DVD or ISO file. Click **Yes** to continue with the installation or **No** to cancel.

Caution   If you choose to continue with the installation, all existing data on your hard drive gets overwritten and destroyed.

The **Platform Installation Wizard** window displays.

Step 7   In the **Platform Installation Wizard** window, choose one of the following options:

- To continue with the basic installation process, choose **Proceed** and continue. Allows you to configure basic installation process.
- If you have a preinstalled server (for example, a Cisco Business Edition server), configure the pre-installed software. Click **Skip** and go to Enter Configuration Information for Preinstalled Servers, on page 33.
- If you want to install the software first and then configure it later, click **Skip**. The installation process installs the software and then prompts you to configure it after the installation is complete. This method may increase the total time for the installation.

Step 8   In the **Apply Additional Release** window, if you have a newer Unified Communications Manager version than your install image, you can elect to upgrade the installation to the newer release. This option is not available for the IM and Presence Service

- **Yes**—Choose this option to upgrade the Unified Communications Manager install image to a newer Service Release. Go to one of the following procedures:

  - Upgrade Install Image from Local Source, on page 34

  - Upgrade Install Image from Remote Server, on page 35

- **No**—Choose this option if you are installing the IM and Presence Service or if you are installing Unified Communications Manager and you do not want to upgrade the install image.

Step 9   In the **Basic Install** window, click **Continue** to install the software or configure the pre-installed software.

What to do next

For pre-installed servers, Enter Configuration Information for Preinstalled Servers, on page 33.

To upgrade the Unified Communications Manager install image to a later release, peform any of the following procedures:

- Upgrade Install Image from Local Source, on page 34

- Upgrade Install Image from Remote Server, on page 35

To continue the basic install process, Configure Basic Installation, on page 37.

Enter Configuration Information for Preinstalled Servers

Use this procedure if you have a server with the product pre-installed (for example, a Cisco Business Edition appliance). You can use a USB key or AFG file to enter your server's pre-configured information.

Before you begin

Basic Installation, on page 32

Procedure

Step 1	After the system restarts, the **Preexisting Installation Configuration** window displays.
Step 2	If you have preexisting configuration information that the Answer File Generator created, that is stored on a USB key. Insert the USB key and choose **Continue**. The installation wizard reads the configuration information during the installation process.

> **Note**   If a popup window states that the system detected new hardware, press any key and then choose **Install** from the next window.

Step 3	In the **Platform Installation Wizard** window, choose **Proceed**.
Step 4	In the **Apply Additional Release** window, you can choose the option to upgrade Unified Communications Manager install file to a newer release. This option is not available for the IM and Presence Service.

- **Yes**—Choose this option to upgrade the Unified Communications Manager install image to a newer Service Release. Go to one of the following procedures:

  > Upgrade Install Image from Local Source, on page 34
  > Upgrade Install Image from Remote Server, on page 35

- **No**—Choose this option if you are installing the IM and Presence Service or installing Unified Communications Manager and you do not want to upgrade the install image.

Step 5	In the **Basic Install** window, choose **Continue**.

What to do next

To upgrade the Unified Communications Manager install image to a newer release, perform any of the following procedures:

- Upgrade Install Image from Local Source, on page 34

- Upgrade Install Image from Remote Server, on page 35

Otherwise, to continue the basic install process, Configure Basic Installation, on page 37

Upgrade Install Image from Local Source

Use this optional procedure for Unified Communications Manager installations if you have a newer version than your installation image and you want to upgrade your installation file to a newer version. This option is available for Unified Communications Manager installs only.

> **Note**   If you have placed your upgrade file on an FTP or SFTP server, refer to Upgrade Install Image from Remote Server, on page 35.

Before you begin

Make sure to do the following:

Note

To complete this procedure, you must have completed the Start Basic Installation procedure and have chosen to apply a patch via a LOCAL source.

- Start a basic installation. Choose the option to apply apatch via a LOCAL source. For details, see

- Download the appropriate patch file from Cisco.com. You must create an ISO image from the upgrade file and then either place it on a DVD or in the DVD drive of a virtual machine.

Procedure

Step 1   When the **Local Patch Configuration** window displays, enter the patch directory and patch name, if required, and choose **OK.**

The **Install Upgrade Patch Selection Validation** window displays.

Step 2   The window displays the patch file. To update the system with this patch, click **Continue**.

Step 3   Choose the upgrade patch to install. The system installs the patch, then restarts the system with the upgraded software version running.

After the system restarts, the **Preexisting Configuration Information** window displays.

Step 4   To continue the installation, choose **Proceed.**

The **Platform Installation Wizard** window displays.

Step 5   To continue the installation, click **Proceed** or click **Cancel** to stop the installation.

If you click **Proceed**, the **Apply Patch** window displays. Continue with the next step.

If you click **Cancel**, the system halts, and you can safely power down the server.

Step 6   When the **Apply Patch** window displays, choose **No.**

Step 7   The **Upgrade** window displays.

Step 8   Click **No** and perform the procedure to configure the basic installation.

What to do next

Upgrade Install Image from Remote Server

Use this optional procedure for Unified Communications Manager installations if you have a newer version than your installation image on an FTP or SFTP server and you want to upgrade your installation file to a newer version. This option is available for Unified Communications Manager installs only.

> ✎ **Note** If you have placed your upgrade file on an FTP or SFTP server, refer to Upgrade Install Image from Local Source, on page 34.

Procedure

Step 1 Configure the auto negotiation setting.

- To enable automatic negotiation, choose **Yes**. This option sets the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. The **MTU Configuration** window displays. Skip the next step then continue.

  Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays. Continue with the next step.

Step 2 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The **MTU Configuration** window displays.

Step 3 In the **MTU Configuration** window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value.

Caution If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), choose **No.**

- To change the MTU size from the operating system default, choose Yes, enter the new MTU size, and choose **OK.**

The **DHCP Configuration** window displays.

Step 4 For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The installation process attempts to verify network connectivity.

- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 5 If you chose not to use DHCP, enter your static network configuration values and choose **OK**.

The **DNS Client Configuration** window displays.

Step 6 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**.

After the system configures the network and checks for connectivity, the Remote Patch Configuration window displays.

Step 7 Enter the location and login information for the remote file server. The system connects to the remote server and retrieves a list of available upgrade patches.

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

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

The **Install Upgrade Patch Selection** window displays.

Step 8 Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system with the upgraded software version running.

After the system restarts, the **Preexisting Configuration Information** window displays.

Step 9 To continue the installation, choose **Proceed.**

The **Platform Installation Wizard** window displays.

Step 10 Choose **Proceed** or Choose **Cancel** to stop the installation.

If you choose **Proceed**, the **Apply Patch** window displays. Continue with the next step.

If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 11 In the **Apply Patch** window displays, choose **No.**

The **Windows Upgrade** window displays.

Step 12 Choose **No** and perform the configure basic installation procedure to configure the basic installation.

What to do next

Configure Basic Installation

Use this procedure to configure Unified Communications Manager and IM and Presence Service basic installation.

Before you begin

Procedure

Step 1 In the **Timezone Configuration** window, choose the appropriate time zone for the server and then choose **OK**.

The **Auto Negotiation Configuration** window is displayed.

Step 2 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**.

  The **MTU Configuration window** is displayed.

  Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No** and continue with the next step.

  The **NIC Speed and Duplex Configuration** window is displayed.

Step 3 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The **MTU Configuration** window displays.

Step 4 In the **MTU Configuration** window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

Caution If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), choose **No.**

- To change the MTU size from the operating system default, choose Yes, enter the new MTU size, and choose **OK.**

The **DHCP Configuration** window displays.

Step 5 For network configuration, you can choose to either set up a static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The network restarts, and the **Administrator Login Configuration** window is displayed.

- If you want to configure a static IP address for the node, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**.

The **DNS Client Configuration** window is displayed.

Step 7 In the **DNS Client Configuration** window, click **Yes** to enable DNS and enter the DNS client information.

Step 8 Click **OK** and choose one of the following in the Basic Installation procedure:

- **Proceed:**

  - Click **Proceed** to restart the network using the new configuration. The **Administrator Login Configuration** window is displayed.

  - Enter Administrator login **User Name** and **Password**

Note	Make sure that the **User Name** contians alphanumeric characters. Use the same login cerdentials to Cisco Unified Communications Operating System Administration, the Command Line Interface, and the Disaster Recovery System.

- **Software Location of Data to Import**

    - Enter Remote Server Name or IP, Export Data Directory, Remote Login ID, Remote Password, and Confirm Password. Click **OK** to restart the network using the new configuration.

Step 9	The **Certificate Information** window is displayed.
Step 10	In **Certificate Information** window, enter your certificate signing request information and click **OK.**
Step 11	In the **First Node Configuration** window, choose how you want to assign this node:

- **Yes**—Choose this option to assign this node as the Cisco Unified Communications Manager publisher node.
- **No**—Choose this option to assign this node as a Cisco Unified Communications Manager subscriber node, or as an IM and Presence Service node.

What to do next

If you are installing the first node in the cluster, go to one of the following procedures, depending on whether you are installing Unified Communications Manager or the IM and Presence Service.:

Configure the Unified Communications Manager Publisher

Follow this procedure to configure the first server where you install Unified Communications Manager software as the publisher node for the cluster. Perform this procedure after you have completed the basic installation and configured the basic installation.

Note	You can configure Smart Call Home on the publisher node only. For more information on Smart Call Home, refer to Smart call home section in the Cisco Unified Serviceability Administration Guide.

Procedure

Step 1	The **Network Time Protocol Client Configuration** window appears.

Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher node. Subscriber nodes in the cluster will get their time from the first node.

Step 2	Choose whether you want to configure an external NTP server or manually configure the system time.

- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose **Proceed** to continue with the installation.

  The system contacts an NTP server and automatically sets the time on the hardware clock.

  Note If the **Test** button appears, you can choose **Test** to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The **Database Access Security Configuration** window appears.

Step 3 Enter the Security password from Required Installation Information.

Note The Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between nodes, and you must ensure this password is identical on all nodes in the cluster.

The **SMTP Host Configuration** window appears.

Step 4 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name. If you do not want to configure the SMTP server, choose **No**, which redirects to Smart Call Home page. To go to previous page, choose **Back** and to see the information about the SMTP configuration, choose **Help**.

Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.

Step 5 Choose **OK**.

Step 6 In the **SMART Call Home Enable** window, choose one of the following and click **OK**:

- **Enable Smart Call Home on System Start**
- **Enable Anonymous Call Home on System Start**
- **Remind me Later to configure Smart Call Home**—Select this option to configure the Smart Call Home feature service after installation using the Cisco Unified Serviceability interface.
- **Disable All Call Home on System Start**—Select this option to deactivate the Smart Call Home feature service. Please note that you can reactivate it after installation using the Cisco Unified Serviceability interface.

Step 7 If you have selected **Smart Call Home on System Start**, do the following:

a) Select the method for sending data to the Cisco Technical Assistance Center.

- Secure Web (HTTPS)

- Secure Web (HTTPS) through Proxy—If you select this option, enter the Hostname or IP address of the proxy server where the Call Home info gets sent as well as the port number on which the server is enabled.

- Email—If you select this option, you must have configured SMTP for any emails to be sent successfully.

b) To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.

c) In the **Customer Contact Details** field, enter the customer's email address.

d) Click **Continue** to proceed, or select **Back** to return to the previous menu.

If you click **Continue**, a message appears as `Cisco Call Home includes reporting capabilities that allow Cisco to receive diagnostic and system information from your Unified Communications Manager cluster. Cisco may use this information for proactive debugging, product development or marketing purposes. To learn more about this feature, please visit: http://www.cisco.com/en/US/products/ps7334/serv_home.html.`

> **Note**   If you have selected **Secure Web (HTTPS) through Proxy** and click **Continue**, the **Smart Call Home Proxy Configuration** window appears.

e) Click **Confirm** to proceed with normal installation or select **Back** to return to the Smart Call Home Enable Page.

Step 8   If you have selected **Enable Anonymous Call Home on System Start**, do the following:

a) Select the method for sending data to the Cisco Technical Assistance Center.

   • Secure Web (HTTPS)

   • Secure Web (HTTPS) through Proxy—If you select this option, enter the Hostname or IP address of the proxy server where the Call Home info gets sent as well as the port number on which the server is enabled.

   • Email—If you select this option, you must have configured SMTP for any emails to be sent successfully.

b) To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.

c) Click **Continue** to proceed, or click **Back** to return to the previous menu.

When you click **Continue**, the following message appears.

`To help improve the Unified Communications Manager experience, click Confirm to allow Cisco Systems to securely receive usage statistics from the server. This information will be used by Cisco to help understand how customers are using our product and ultimately drive product direction. If you prefer not to participate, you may choose to opt-out.`

> **Note**   If you have selected **Secure Web (HTTPS) through Proxy** and clicked **Continue**, the **Anonymous Call Home Proxy Configuration** window appears.

d) Click **Confirm** to proceed with normal installation or click **Back** to return to the Smart Call Home Enable Page.

Step 9   Click **OK**. The **Application User Configuration** window appears.

Step 10   Enter the Application User name and password from and confirm the password by entering it again.

Step 11   Choose **OK**.
The Platform Configuration Confirmation window appears.

Step 12   Choose **OK** to continue with the installation or choose **Back** to modify the platform configuration.

The system installs and configures the software. The server reboots.

When the installation process completes, you are prompted to log in by using the Administrator account and password.

What to do next

If you want to install subscriber nodes, Add Subscriber Nodes, on page 42.

Configure the IM and Presence Publisher

Follow this procedure to configure the first server where you install IM and Presence Service software as the database publisher node for the IM and Presence cluster.

Procedure

Step 1 Install and configure the IM and Presence database publisher node.

Step 2 Verify that the following services are running:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

If you need to activate services, you can do it in Cisco Unified Serviceability at **Tools** > **Service Activation**.

What to do next

Add Subscriber Nodes, on page 42

Add Subscriber Nodes

Before you install software on your subscriber nodes, you must add the subscriber nodes to the Unified Communications Manager publisher node. You must complete this task before installing subscriber nodes for either Unified Communications Manager or the IM and Presence Service.

Procedure

Step 1 Log in to the Unified Communications Manager publisher node.

Step 2 From Cisco Unified CM Administration choose **System** > **Server**.

Step 3 Add your subscriber nodes:

a) Click **Add New**.

b) From the **Server Type** drop-down list, choose the node type that corresponds to the install that you are completing: Unified Communications Manager Voice/Video node, or IM and Presence node.

c) Enter the **Fully Qualified Domain Name/IP Address** field with a FQDN or IPv4 Address.

> **Note** Do not use single quotes (' ') in the Description field while adding the node details.

    d) Optional. If you are deploying IPv6, enter an **IPv6 Address**.

    e) Click **Save**.

    f) Repeat these steps for each subscriber node that you want to add.

Step 4   (IM and Presence Service only) Add your Presence Redundancy Groups in order to define your subclusters.

    a) From Cisco Unified CM Administration, choose **System** > **Presence Redundancy Groups**.

    b) Click **Add New**.

    c) Enter a **Name** and **Description** for the group.

    d) From the **Server** drop-down list, choose the IM and Presence nodes that you want to add to this group.

    e) Click **Save**.

    f) Repeat this procedure until you've created your groups. You can have up to three Presence Redundancy Groups in a cluster, with each group consisting of two IM and Presence nodes.

What to do next

Install Subscriber Nodes

Use this procedure if you want to install subscriber nodes for Unified Communications Manager or the IM and Presence Service.

Before you begin

Before you install software for either Unified Communications Manager or IM and Presence Service subscriber nodes, you must add the node to the Cisco Unified Communications Manager publisher node. For details,

Procedure

Step 1   If you have configured Network Time Protocol on the publisher node, ensure that it is synchronized with an NTP server before you install a subscriber node. From the Command Line Interface on the publisher node, enter `utils ntp status`. Ensure that the output indicates that the node is synchronized with an NTP server.

> **Note** If the publisher node is not synchronized with an NTP server, installation of the subscriber node will fail.

Step 2   On the First Node Configuration window, read the Warning and make sure that you have correctly configured the first node as the publisher node. To continue with the installation of the subscriber node, click **OK.**

The Network Connectivity Test Configuration window displays.

Step 3   During installation of a subscriber node, the system checks to ensure that the subscriber node can connect to the publisher node.

      • To pause the installation after the system successfully verifies network connectivity, choose **Yes.**

> • To continue the installation with a pause, choose **No.**

The First Node Access Configuration window displays.

Step 4   Enter the publisher node connectivity information and choose **OK.**

The system checks for network connectivity.

If you chose to pause the system after the system successfully verifies network connectivity, the Successful Connection to First Node window displays. Choose **Continue.**

Note   If the network connectivity test fails, the system always stops and allows you to go back and reenter the parameter information.

The **SMTP Host Configuration** window displays.

Step 5   If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

Note   To use certain operating system features, you must configure an SMTP server; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface.

The Platform Configuration Confirmation window displays.

Step 6   Choose **OK** to start installing the software or choose **Back** to change the configuration.

Step 7   When the installation process completes, you get prompted to log in by using the Administrator account and password.

What to do next

If you have just installed a Unified Communications Manager cluster and you want to install the IM and Presence Service on the same cluster in a standard IM and Presence deployment (as opposed to a central IM and Presence cluster deployment), return to Basic Installation, on page 32 in order to install the IM and Presence Service cluster.

Otherwise, proceed to the postinstallation tasks:

- Postinstall Tasks for Cisco Unified Communications Manager, on page 53
- Postinstall tasks for the IM and Presence Service, on page 64

Touchless Installation Task Flow

Complete these tasks to install your Unified Communications Manager and IM and Presence Service clusters in a single process via the touchless installation method.

Before you begin

Preinstall Tasks for Cisco Unified Communications Manager, on page 21

Preinstall Tasks for the IM and Presence Service, on page 23

Procedure

	Command or Action	Purpose
Step 1	Generate Answer Files for Touchless Install, on page 45	Use this procedure to generate the configuration files (clusterconfig.xml and platformconfig.xml) with your network settings. The touchless install process uses these files to install and configure the various cluster nodes.
Step 2	Generate Virtual Floppy Images, on page 46	Use this procedure to create virtual floppy images from the answer files. You will use the virtual floppy images in your touchless installation.
Step 3	Upload Virtual Floppy Image to Datastore, on page 47	Use this procedure to upload the virtual floppy images to the datastore.
Step 4	Mount Floppy Image to VM, on page 48	Use this procedure to mount the UC application virtual floppy images on their corresponding VM.
Step 5	Run Touchless Install, on page 48	Begin the cluster installation. You can kick off all node installations simultaneously.

Generate Answer Files for Touchless Install

Use this procedure to generate answer files for your touchless installation of your cluster. The answer files (clusterconfig.xml and platformconfig.xml) contain the configuration information that the install process installs and configures on each cluster node.

Before you begin

You must have already planned your network topology, including addresses for your Unified Communications Manager and IM and Presence Service cluster nodes.

Procedure

Step 1   Log in to the Cisco Unified Communications Answer File Generator application at https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html.

Step 2   In the **Hardware** section, choose **Virtual Machine**.

Step 3   From the **Product** section, select the product and version that you want to install.

Step 4   Complete the remaining fields under **Clusterwide Configuration** with your cluster configuration details.

Note   **Software Location of Data to Import** section applicable for the destination release 14 and above and if you choose to **Fresh Install with Data Migration** else ignore this section. Check the **Configure Software Location of Data to Import** check box to configure Remote SFTP server details and generate files for the UCM cluster to execute **Fresh Install with Data Migration**. By checking the above check box it disables, **Administrator Credentials, Security Password, Application User Credentials** fields. These details are imported from source node data during installation. Enter the following option:

Table 3:

Field	Description
Remote Server Name or IP	The Secure FTP (SFTP) server that will store the source cluster's exported data
Export Data Directory	Directory path on the server containing export data
Remote Server Login ID	Allow for data retrieval of the remote SFTP server
Remote Server Password	Contains alphanumeric characters, hyphens, and underscores

Step 5   Complete the fields in the **Primary Node Configuration** with configuration details for the publisher node.

Step 6   Check the **Dynamic Cluster Config Enable** check box and enter a value, in hours, for the Dynamic cluster Config Timer.

Note   This check box must be checked if you want to install your full cluster in a single process. Otherwise, you will need to either configure this option later through the CLI, or add your subscriber nodes manually after the publisher node installs.

Step 7   Under **Secondary Node Configuration**, enter the node details for your first subscriber node and click **Add Secondary Node**.

Step 8   Add all of your subscriber nodes.

Step 9   Add all your cluster notes and click **Generate Answer files**.

Step 10   Download the answer files to your computer.

Step 11   Repeat this procedure to generate answer files for the IM and Presence Service cluster.

What to do next

Generate Virtual Floppy Images

Use this procedure to create virtual floppy images from the answer files. You will use the virtual floppy images in your touchless installation.

Note　This procedure describes how to use Winimage to create virtual floppy images. You can download Winimage from http: www.winimage.com download.htm. You can also use other tools, such as BFI, to create virtual floppy images.

Procedure

Step 1　From Winimage, choose **File** > **New**.

Step 2　From the Standard format, choose **1.44 MB** and click **OK**.

Step 3　Navigate to the Menu Image, choose **Inject** and select the `platformConfig.xml` file.

Step 4　When prompted to inject the file into Winimage, click **Yes**.

Step 5　Choose **File** > **Save As**.

Step 6　Save the file as a virtual floppy image (.flp file) using the following naming conventions:

- Unified Communications Manager—`ucm.flp`
- IM and Presence Service—`imp.flp`

Step 7　Repeat these steps for both the Unified Communications Manager cluster and the IM and Presence Service cluster.

What to do next

Upload Virtual Floppy Image to Datastore

Use this procedure to upload the virtual floppy images to the datastore.

Procedure

Step 1　Start the vSphere client.

Step 2　Select the **Configuration** tab.

Step 3　Select **Storage**.

Step 4　Right-click on a datastore and **Browse** the datastore.

Step 5　Navigate to the destination directory and click the **Upload files to this datastore** icon.

Step 6　Upload the vFloppy images to the AFG folder.

Step 7　At the **Upload/Download** warning, click **Yes**.

Step 8　Close the **Datastore Browser** window.

What to do next

Mount Floppy Image to VM

Use this procedure to mount the UC application virtual floppy images on their corresponding VM.

Procedure

Step 1   In the vSphere client, choose the virtual machine.

Step 2   Open VMware Remote Console (VMRC), and click the **Floppy drive**.

Step 3   Select **Use existing floppy image in datastore**.

Step 4   **Browse** to the datastore and locate the virtual floppy image.

Step 5   Select the file and click **OK**.

Step 6   Under **Device Status**, enable the **Connected and Connect at power on** option.

Step 7   Click the **Options** tab. Under **Boot Options**, check **Force entry to BIOS** and click **OK**.

Step 8   Repeat this procedure for each VM on which you want to install a node.

What to do next

Run Touchless Install

After you have mounted your virtual floppy drives to your application VMs, run the touchless installation process. You can install all nodes simultaneously.

Procedure

Step 1   In vSphere client, right-click the **VM** and select **Open Console**. A console window opens.

Step 2   Click the **Power On** icon in the console tool bar to power on the virtual machine.

Step 3   When the BIOS screen appears, configure the following boot order:

a) CD-Rom

b) Hard Drive

c) Removable Devices

d) Network

Step 4   Save the settings and exit from the console. The installation commences immediately.

Step 5   Repeat these steps for each cluster node.

Step 6   After to emphasise the completion of an activity, remove the vFloppy configurations from the virtual machines.

What to do next

Add a New Node to an Existing Cluster

To add a new Unified Communications Manager or IM and Presence Service subscriber node to an existing cluster, you can use either the Basic Installation or Touchless Installation methods to add and install the node. Any new nodes that you add must be configured as subscriber nodes.

Basic Installation

For basic installations of additional Unified Communications Manager or IM and Presence Service cluster nodes, complete the following tasks:

	Procedure	Description
Step 1	Run a full backup of the cluster.	For details, see the "Manage Backups" chapter of the *Administration Guide for Cisco Unified Communications Manager*.
Step 2	Basic Installation, on page 32	Begin the install process.
Step 3	Configure Basic Installation, on page 37	Continue with the Basic Installation process by configuring your installation.
Step 4	Add Subscriber Nodes, on page 42	Add subscriber nodes to Unified Communications Manager publisher.
Step 5	Install Subscriber Nodes, on page 43	Install software on your subscriber nodes.

Touchless Installation

For Touchless installations of additional Unified Communications Manager or IM and Presence Service cluster nodes, complete these tasks:

	Procedure	Description
Step 1	Run a full backup of the cluster.	For details, see the "Manage Backups" chapter of the *Administration Guide for Cisco Unified Communications Manager*.
Step 2	Generate Answer Files for Touchless Install, on page 45	Generate answer files for your installation. The touchless install process uses answer files to install and configure the various cluster nodes.
Step 3	Generate Virtual Floppy Images, on page 46	Create a virtual floppy image from the answer file.

	Procedure	Description
Step 4	Upload Virtual Floppy Image to Datastore, on page 47	Upload the virtual floppy to the datastore.
Step 5	Mount Floppy Image to VM, on page 48	Mount the virtual floppy to the virtual machine.
Step 6	Run Touchless Install, on page 48	Install the software.

Notes for Basic and Touchless Installs

☞

Important After you install a new node on an existing cluster, if you plan to utilize Cisco CallManager or Cisco TFTP services, we recommend that you restart all of the phones in your cluster to get the latest ITL file. If you are using a Certificate Trust List (CTL), you will also need to update this file manually by running the `utils ctl update CTLFile` CLI command (using Tokenless CTL) or by updating the file via the CTL Client (Legacy USB tokens). After you update the CTL file, you must restart phones so that they can download the latest CTL file. For additional details on the CTL File, see the "Cisco CTL Client Setup" chapter of the *Security Guide for Cisco Unified Communications Manager*.

✎

Note
- You can collect the logs from RTMT of a new node added to the existing FQDN cluster, only when you restart the trace collection service. When you sign in to Unified RTMT without restarting the trace collection, the following error message is displayed: .

  ```
  Could not connect to 'Server' <new node name>
  ```

- If you install a new node to an existing cluster where the IM and Presence server is not upgraded to the supported version or if the IM and Presence server has been decommissioned, the following error message is displayed:

  ```
  "Add failed. Upgrade and migration for Cisco Unified IM & Presence
  Servers that are associated with this cluster appears to be pending
  (not complete). Please make sure upgrade and migration of all IM &
  Presence servers is completed successfully before adding servers to
  this cluster. Please check for any unused IM & Presence Application
  Servers and delete them".
  ```

Note A touchless install cannot be used to install multiple Unified Communications Manager and IM and Presence Service nodes simultaneously. The following scenarios are supported:

- Installing multiple Unified Communications Manager nodes

- Installing one Unified Communications Manager node (publisher) and multiple and IM and Presence Service nodes

If you need to install multiple Unified Communications Manager and IM and Presence Service nodes, you need to use one of the above scenarios and install additional nodes manually.

Postinstallation Tasks

Postinstall Tasks for Cisco Unified Communications Manager

Procedure

	Command or Action	Purpose
Step 1	Read the Release Notes and any Readme files that come with your release.	You can download Release Notes from the below URL. Make sure that you understand the features for your release and any COP file requirements. https://www.cisco.com/c/en/us/support/ unified-communications/ unified-communications-manager-callmanager/ products-release-notes-list.html
Step 2	Reset Application User Passwords, on page 54	Cisco recommends that you reset your application user passwords post installation.
Step 3	Install the Real-Time Monitoring Tool, on page 55	You can use the Cisco Unified Real-Time Monitoring Tool (RTMT) to monitor Unified Communications Manager and the IM and Presence Service in real time.
Step 4	Enable the Kerneldump Utility, on page 57	If you have a kernel crash, the kerneldump utility provides a mechanism for collecting and dumping the crash.
Step 5	Install Licenses, on page 57	Verify that you have the required licenses for your system and devices.

	Command or Action	Purpose
Step 6	Configure the Backup, on page 57	Cisco recommends performing regular backups. You can set up automatic backups or invoke a backup at any time.
Step 7	Install New Locales, on page 58	Optional. The default locale is US - English. If you want to use a different locale, download and install it.
Step 8	COP File Installation Guidelines, on page 61	You may need to install a COP file after the installation to fix a known defect, or to enable support for a custom device type that you want to use that does not ship with Unified Communications Manager.
Step 9	Install a dial plan by completing these tasks: • Install a COP File, on page 61 • Install a Prebuilt Dial Plan, on page 62 • Restart the Cisco CallManager Service, on page 62	If you want to use a dial plan other than the North American Numbering Plan (the default), you must download and install it.
Step 10	Activate Security, on page 63	Optional. If you want to enable security on your system, install the Cisco CTL Client and enable mixed mode.
Step 11	Configure the Simple Network Management Protocol, on page 63	Optional. If you are using a Network Management System such as Cisco Prime Collaboration Assurance, enable the Simple Network Management Protocol.
Step 12	Change Virtual Machine Configuration Specifications, on page 64	To change to the Guest OS version in the Cisco Unified Communications Manager virtual machine (VM) settings.

Reset Application User Passwords

The install process sets all Application User passwords to the same default Application User password that you entered during installation. Cisco recommends that you reset all of these passwords post installation.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Find**.

Step 3 Click on an application user.
The details of the application user appear in the **Application User Configuration** window.

Step 4 Enter the new password in both the **Password** and **Confirm Password** fields.

Step 5 Click **Save**.

Step 6   Repeat this procedure for each application user.

Install the Real-Time Monitoring Tool

Use this procedure to install the Cisco Unified Real-Time Monitoring Tool (RTMT). You can use RTMT to monitor Unified Communications Manager and the IM and Presence Service in real time.

Before you begin

- Unified RTMT requires at least 128 MB in memory to run on a Windows OS platform; the tool requires at least 300 MB of disk space to run on a Windows/Linux OS platform.

Note   The Linux Unified RTMT plugin CcmServRtmtPlugin.bin can be installed on RHEL 5, RHEL 6, or higher Linux machines. If you want to install it on a RHEL 4 machine, ensure that the glibc (OS library) version is 2.4.x or higher. If the glibc version is 2.3.x or earlier, the underlying JRE install fails.

- The current Unified RTMT download supports earlier releases of Unified Communications Manager or Cisco Unity Connection. Some releases of Unified Communications Manager may require different versions of Unified RTMT to be installed on your computer (one version per Unified Communications Manager release). Verify that the Unified RTMT version that you install is compatible with the product that you are monitoring. If the Unified RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and Unified RTMT frame size, based on the last instance of Unified RTMT that you run.

Note   Only the administrators with Standard Audit Users and Standard CCM Super Users privileges have access to Unified RTMT features. If an application user without these privileges logs into Unified RTMT, some of the features such as Call Control Discovery (CCD) and Service Advertisement Framework (SAF) will not work as expected.

Note   On a Linux workstation, run RTMT with root access. Otherwise, when you initially install RTMT, the application will not start.

- The current Unified RTMT requires JRE to run. Verify that the system has JRE installed (Java 1.8).

Procedure

Step 1   Go to the **Plug-ins** window of the administration interface for your configuration:

Interface	How to access
Unified Communications Manager	From Unified Communications Manager Administration, choose **Application** > **Plugins**.
Unified Communications Manager IM and Presence Service	From Unified Communications Manager IM and Presence Administration, choose **Application** > **Plugins**.
Cisco Unity Connection	From Cisco Unity Connection Administration, choose **System Settings** > **Plugins**.

Step 2   Click **Find**.

Step 3   To install Unified RTMT on a client that is running the Microsoft Windows operating system, click the **Download** link for the Real-Time Monitoring Tool - Windows.

To install Unified RTMT on a client that is running the Linux operating system, click the **Download** link for the Real-Time Monitoring Tool - Linux.

> **Tip**   When you install Unified RTMT on Windows 7 or later, ensure that you perform the installation as an administrator.

Step 4   Download the executable to the preferred location on your client.

Step 5   To install the Windows version, double-click the Unified RTMT icon that appears on the desktop or locate the directory where you downloaded the file and run the Unified RTMT installation file.

The extraction process begins.

Step 6   To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**.

Step 7   After the Unified RTMT welcome window appears, click **Next**.

Step 8   To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.

Step 9   Choose the absolute path of Java Virtual Machine executable from your system (java.exe from the JRE installed directory, that is latest version 1.8) as prompted in the installation screen of Unified RTMT.

Step 10   Choose the location where you want to install Unified RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Step 11   To begin the installation, click **Next**.

The **Setup Status** window appears.

Step 12   To complete the installation, click **Finish**.

> **Note**   For more details on how to use the Real-Time Monitoring Tool, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump the core to either the local server, or to an external server.

Procedure

Step 1   Log in to the Command Line Interface.

Step 2   Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kernelcrash enable` CLI command.
- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3   Reboot the server.

Install Licenses

Make sure that you acquire the necessary licenses.

Unified Communications Manager Requirements

Use Cisco Smart Software Manager or Cisco Smart Software Manager satellite to manage licenses for Unified Communications Manager. For details on how to acquire licenses, see the "Smart Software Licensing" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

IM and Presence Service Requirements

The IM and Presence Service does not require a server license or software version license.

Configure the Backup

Cisco recommends performing regular backups. You can use the Disaster Recovery System (DRS) to do a full data backup for all servers in a cluster. You can set up automatic backups or invoke a backup at any time.

You can initiate a manual backup or configure a backup schedule. For more details, see the "Backup the System" chapter of the *Administration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Locale Installation

You can configure Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale

installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

For upgrades of Unified Communications Manager or the IM & Presence Service, you must install locales after you have completed all of your upgrades and migrations. For upgrades, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Install the latest version of the locales that match the major.minor version number of your Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Unified Communications Manager locale file for the same country on the Unified Communications Manager cluster.

Use the information in the following sections to install locales on Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:

- `cm-locale-language-country-version.cop` (Unified Communications Manager)

- `ps- locale-language_country-version.cop` (IM and Presence Service)

Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- `cm-locale-combinednetworklocale-version.cop` (Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Install New Locales

Use this procedure to install a new locale on Unified Communications Manager or IM and Presence Service. If you are installing a locale for both products, install the locale on all cluster nodes in the following order:

1. Unified Communications Manager publisher node

2. Unified Communications Manager subscriber nodes

3. IM and Presence database publisher node

4. IM and Presence subscriber nodes

Before you begin

Make sure that you have completed your installation or upgrade of Unified Communications Manager or IM and Presence Service on all cluster nodes before you attempt to install a new locale.

Procedure

Step 1 Find the locale installer for your release on cisco.com:

- For Unified Communications Manager, go to https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm
- For IM and Presence Service, go to https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm

Step 2 Download your release's locale installer to a server that supports SFTP.

Step 3 Log in to Cisco Unified OS Administration using the administrator account.

Step 4 Choose **Software Upgrades** > **Install/Upgrade**.

Step 5 Complete the following fields in the **Software Installation/Upgrade** window:

- For the **Source**, choose **Remote file System**.
- From the **Directory**, enter the path to the directory where you saved the locale installer.
- From the **Server** field, enter the server name for the remote file system.
- Enter the credentials for the remote file system.
- From the **Transfer Protocol** drop-down list, choose **SFTP**. You must use SFTP for the transfer protocol.

Step 6 Click **Next**.

Step 7 Download and install the locale on the server.

Step 8 Restart the server. The updates take effect after the server restarts.

Step 9 Repeat this procedure on all Unified Communications Manager and IM and Presence Service cluster nodes in the prescribed order.

Note Do not reset user locales for your end users until the new locale is installed on all cluster nodes. If you are installing the locale for both Unified Communications Manager and IM and Presence Service, you must install the locale for both products before you reset user locales. If you run into any issues, such as could occur if an end user resets a phone language before the locale installation is complete for IM and Presence Service, have your users reset their phone language in the Self-Care Portal to English. After the locale installation is complete, users can reset their phone language, or you use Bulk Administration to synchronize locales to the appropriate language by bulk.

What to do next

After the locale installation is complete for all cluster nodes, your end users can begin using the new user locale.

Error Messages

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 4: Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database. This indicates an error with the build process.
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable.	This error occurs because a Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Unified Communications Manager database. If this application is not found, it either was not installed with Unified Communications Manager (very unlikely), has been deleted (more likely), or the node does not have Unified Communications Manager installed (most likely). Installation of the locale terminates because locales do not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale /cmservices/ipma/com/cisco/ipma /client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/ application_locale/cmservices/ipma/com/cisco/ ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/ application_locale/cmservices/ipma/ LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, /usr/local/thirdparty/java/j2sdk/ jre/bin/java, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Unified Communications Manager Assistant, which cannot detect a change in localized Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMaster Version.txt in order to update UnifiedCMAssistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.

Message	Description
[LOCALE] Addition of <RPM-file-name> to the Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

COP File Installation Guidelines

Depending on your installation, you may need to install a COP file after the installation to fix a known defect, or to enable support for a custom device type that you want to use that does not ship with Unified Communications Manager.

If you need to install a COP file, follow these guidelines:

- Install the appropriate COP file on every node in a cluster. Perform this task before you install new software on each node in the cluster and after set up the database.

- After you install a COP file, you must restart the node.

- Restart Unified Communications Manager and/or the IM and Presence Service to ensure that configuration changes that are made during the COP file installation get written into the database.

Install a COP File

If you want to use a prebuilt Dial Plan other than the North American Numbering Plan (the system default), you must install a COP file with your dial plan.

Procedure

Step 1 Begin this procedure on the Unified Communications Manager publisher node. From Cisco Unified Communications OS Administration, choose **Software Upgrades** > **Install**.
The **Software Installation/Upgrade** window appears.

Step 2 In the **Source** field, choose **Remote File System**.

Step 3 Configure the fields on the **Software Installation/Upgrade** window. See the Related Topics for more information about the fields and their configuration options.

Step 4 Click **Next**.
The window refreshes with a list of available software options and upgrades.

Step 5 From the **Options/Upgrades** drop-down list, choose the **DP COP** file and click **Next**.
The **Installation File** window opens and downloads the file from the FTP server. The window displays the progress of the download.

Step 6 When the **Checksum** window appears, verify the checksum value against the checksum for the file that you downloaded.

Step 7 Click **Next** to proceed with the software upgrade.
A warning message displays the DP COP file that you selected to install.

Step 8 Click **Install**.
The **Install Status** window appears.

Step 9 Click **Finish**.

Step 10   Repeat this procedure on the Unified Communications Manager subscriber nodes. You must install the COP file on all the nodes in the cluster.

What to do next

To apply the dial plan to the system, Install a Prebuilt Dial Plan, on page 62.

Install a Prebuilt Dial Plan

Install the national numbering plan on each Unified Communications Manager node in the cluster beginning. Begin with the Unified Communications Manager publisher node.

Note   Complete this procedure only if you are installing a national numbering plan for countries outside of North America (the system default).

Before you begin

Install a COP file with your prebuilt dial plan. For details, see Install a COP File, on page 61.

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Dial Plan Installer**.

Step 2   Enter search criteria and click **Find**.

Step 3   Choose the dial plan version that you want to install from the **Available Version** drop-down list.

Step 4   Click **Install**.
The Status displays that the dial plan has been installed.

Step 5   Repeat this procedure for every subscriber node in the cluster.

What to do next

Restart the Cisco CallManager Service, on page 62

Restart the Cisco CallManager Service

If you have installed a new dial plan, you must restart the Cisco CallManager service.

Procedure

Step 1   From the Cisco Unified Serviceability interface, choose **Tools** > **Control Center - Feature Services**.

Step 2   Choose the Unified Communications Manager server from the **Servers** drop-down list.
In the CM Services area, Cisco CallManager displays in the **Service Name** column.

Step 3   Click the radio button that corresponds to the Cisco CallManager service.

Step 4   Click **Restart**.
The service restarts and displays the message, `Service Successfully Restarted.`

Activate Security

If you want to enable security on your system, you must install the Cisco CTL Client and enable mixed mode. You can download the CTL installation file in Cisco Unified CM Administration from the **Applications** > **Plugins** window.

When mixed mode is enabled, the system uses the Certificate Trust List (CTL) file for authentication. The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

For details on how to install the CTL client and enable mixed mode on your system, refer to the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/ unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configure the Simple Network Management Protocol

If you are using a Network Management System, such as Cisco Prime Collaboration Assurance, enable the Simple Network Management Protocol.

Before you begin

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

Procedure

Step 1   Install and configure the SNMP NMS.

Step 2   In the **Control Center - Network Services** window, verify that the system started the SNMP services.

Step 3   Unified Communications Manager: In the **Service Activation** window, activate the Cisco CallManager SNMP service. Cisco Unity Connection only: The Connection SNMP Agent service automatically activates.

Step 4   If you are using SNMP V1/V2c, configure the community string.

Step 5   If you are using SNMP V3, get the SNMP Engine. You will need it when configuring an SNMP User

Step 6   If you are using SNMP V3, configure the SNMP user.

Step 7   Configure the notification destination for traps or informs.

Step 8   Configure the system contact and location for the MIB2 system group.

Step 9   Configure trap settings for CISCO-SYSLOG-MIB.

Step 10   Unified Communications Manager only: Configure trap settings for CISCO-CCM-MIB.

Step 11   Restart the Primary Agent service.

Step 12   On the NMS, configure the Unified Communications Manager trap parameters.

Change Virtual Machine Configuration Specifications

Use the following procedure to change to the Guest OS version in the Cisco Unified Communications Manager virtual machine (VM) settings.

Procedure

Step 1 Shut down the virtual machine.

Step 2 Change the configuration of the virtual machine as needed through vSphere. You can update the Guest OS and VM Hardware Compatibly.

a. Update VM Hardware Compatibly - Left click Virtual Machine. Check for *Updates*. Click **Update**

   Note If you are not aware of the host click **Check statuts** and click **Upgrade** to match host.

b. Update Guest OS - Right click on **Virtual Machine** > **Edit Settings** > **Virtual Machine Option** > **General Option** > **Guest OS Version**.

Step 3 Power on the Virtual Machine.

   Note Following warning messages appears in ESXi while opening the Virtual Machine settings while running when there is a mismatch.

   Warning The configured guest OS (CentOS 4/5 or later (64 bit)) for this virtual machine does not match the guest that is currently running (CentOS 7 (64 bit)). You should specify the correct guest OS to allow for guest-specific optimizations.

Postinstall tasks for the IM and Presence Service

If you have installed a new cluster or new node for the IM and Presence Service, complete these tasks after your installation.

Note Many of these tasks are documented in more detail in the *System Configuration Guide for the IM and Presence Service*. Where indicated, refer to that guide for detail on how to complete these tasks.

Procedure

	Command or Action	Purpose
Step 1	Read the Release Notes and any Readme files that come with your release.	You can download Release Notes from the below URL. Make sure that you understand the features for your release and any COP file requirements.

	Command or Action	**Purpose**
		https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html
Step 2	Check for software and firmware updates for IM and Presence Service on Cisco.com.	You can download software from https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm
Step 3	Configure Presence Redundancy Groups.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 4	Change the default domain.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 5	Change the IM and Presence Service IM address scheme.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 6	Change the IM and Presence Service node name.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 7	Configure Unified Communications Manager as a Presence Gateway.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 8	Configure a SIP Publish trunk on Unified Communications Manager.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 9	Assign users to servers.	For details, see the *System Configuration Guide for the IM and Presence Service*.
Step 10	Activate services, on page 65	Turn on essential IM and Presence services.

Activate services

You must activate the following services:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

To activate the services, select **Tools** > **Service Activation** in Cisco Unified Serviceability.

✎

Note   You must complete this task on each server that you install in an IM and Presence cluster.

Where to Go Next

You have now installed your system. You are now ready to proceed with configuring your system, including tasks such as configuring the dial plan, provisioning users, registering devices, and setting up instant messaging and presence. Refer to the following documents for details on how to configure your system.

- *System Configuration Guide for Cisco Unified Communications Manager*

- *System Configuration Guide for the IM and Presence Service*

You can find these documents at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Troubleshooting

- Network Errors During Installation, on page 67
- Failed Installations, on page 67
- Unrecoverable IM and Presence Service Node, on page 68

Network Errors During Installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If it cannot connect, a message displays, and you get prompted to select one of the following options:

- —RETRY - The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.

- —REVIEW (Check Install) - This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows.

- Networking gets validated after you complete each networking window, so the message might display multiple times.

- —HALT - The installation halts. You should use the Recovery CD to recover the logs to access the diagnostic information. For more details, see Obtain and Run Recovery Software on the CUCM VM.

  > **Note**   We no longer support the collection of logs by dumping them to serial port due to CentOS limitations.

- —IGNORE - The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box might display multiple times. If you choose to ignore network errors, the installation may fail.

Failed Installations

If your installation fails, check the configuration and confirm the following:

- Parse the passwords from the platformconfig.xml file to verify security password.

- Complete a packet capture from Unified Communications Manager to confirm that the IM and Presence Service IP address is reaching Unified Communications Manager during the install.

- Verify that NTP is synchronized on Unified Communications Manager.

- If you get a message that install has failed and you want to recover the logs to access the diagnostic information, see Obtain and Run Recovery Software on the CUCM VM.

> **Note** We no longer support the collection of logs by dumping them to serial port due to CentOS limitations.

- Confirm that the version of the IM and Presence Service and Unified Communications Manager are compatible.

- If you are installing a subscriber, verify that the subscriber node is the same version as the publisher node. The subscriber OVA should be the same OVA that is used for the publisher.

Unrecoverable IM and Presence Service Node

If a node is in a state that cannot be recovered you must reinstall the node.

> **Note** If you reinstall a node in an intercluster deployment, you must delete and re-add the intercluster peer connections between the reinstalled node and the other nodes in the cluster.

IM and Presence Service Database Publisher Node

Complete the following high-level procedure to reinstall an IM and Presence Service database publisher node.

> **Note** If you do not complete all of these steps in the order shown, recovery of the IM and Presence Service database publisher node will fail.

1. Power down all the IM and Presence Service subscriber nodes.

2. Delete the subscriber nodes as follows:

   a. Unassign all users that are assigned to each of the IM and Presence Service subscriber nodes. (Select **Cisco Unified CM Administration** > **User Management** > **Assign Presence Users**).

   b. Remove the subscriber nodes from their presence redundancy groups. (Select **Cisco Unified CM Administration** > **System** > **Presence Redundancy Groups**).

   c. Delete the subscriber nodes from the Unified Communications Manager server list. (Select **Cisco Unified CM Administration** > **System** > **Server**).

3. Power down the IM and Presence Service database publisher node.

4. Delete the IM and Presence Service database publisher node as follows:

  a. Unassign the users that are assigned to the IM and Presence Service database publisher node. (Select **Cisco Unified CM Administration** > **User Management** > **Assign Presence Users**).

  b. Remove the node from the presence redundancy group. (Select **Cisco Unified CM Administration** > **System** > **Presence Redundancy Groups**).

  c. Delete the IM and Presence Service database publisher node from the Unified Communications Manager server list. (Select **Cisco Unified CM Administration** > **System** > **Server**).

5. Readd the IM and Presence Service database publisher node to the Unified Communications Manager server list.

6. Perform a fresh install of the IM and Presence Service database publisher node.

7. Readd the IM and Presence Service subscriber nodes to the Unified Communications Manager server list.

8. Perform a fresh install of each subscriber node.

IM and Presence Service Subscriber Node

Complete the following high-level procedure to reinstall an IM and Presence Service subscriber node.

Note   If you do not complete all of these steps in the order shown, recovery of the IM and Presence Service subscriber node will fail.

1. Power down the IM and Presence Service node.

2. Delete the subscriber node as follows:

  a. Unassign the users that are assigned to the node. (Select **Cisco Unified CM Administration** > **User Management** > **Assign Presence Users**).

  b. Remove the node from the presence redundancy group. (Select **Cisco Unified CM Administration** > **System** > **Presence Redundancy Groups**).

  c. Delete the node from the Unified Communications Manager server list. (Select **Cisco Unified CM Administration** > **System** > **Server**)

3. Readd the IM and Presence Service node to the Unified Communications Manager server list.

4. Perform a fresh install of the node.