



## **Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 14SU2**

**First Published:** 2022-06-16

**Last Modified:** 2024-02-26

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### Full Cisco Trademarks with Software License ?

---

#### CHAPTER 1

#### **New and Changed Information 1**

New and Changed Information 1

---

#### CHAPTER 2

#### **Planning the Installation 3**

Topology Options 3

Cluster Topology for IM and Presence 4

Installation Methods 5

Requirements and Limitations 10

Subnet Limitations 11

Cluster Size 11

IP Address Requirements 11

DNS requirements 11

Firewall Requirements 12

Platform Requirements 12

Supported Versions 13

Software Restrictions 13

Username and Password Requirements 13

    Password Recommendations 15

Installation Time Requirements 16

Licensing Requirements 16

    Unified Communications Manager License Requirements 17

    IM and Presence Service License Requirements 18

Required Installation Information 19

Export Restricted and Export Unrestricted Software 24

---

**CHAPTER 3**

**Preinstallation Tasks 27**

- Preinstall Tasks for Unified Communications Manager 27
- Preinstall Tasks for the IM and Presence Service 29
- Enable the Cisco AXL Web Service 30
- Verify DNS Registration 31

---

**CHAPTER 4**

**Installation Methods 33**

- Installation Methods Task Flows 33
  - Installation Wizard Considerations 34
- Attended Installation Task Flow 35
  - Install IM and Presence Central Cluster (Attended Installation) 36
    - Attended Installation 37
    - Upgrade Install Image from Local Source 39
    - Upgrade Install Image from Remote Server 40
    - Configure Attended Installation 42
    - Configure the Unified Communications Manager Publisher 44
    - Configure the IM and Presence Publisher 47
    - Add Subscriber Nodes 47
    - Install Subscriber Nodes 48
- Touchless Installation Task Flow 49
  - Generate Answer Files for Touchless Install 50
  - Generate Virtual Floppy Images 51
  - Upload Virtual Floppy Image to Datastore 52
  - Mount Floppy Image to VM 52
  - Run Touchless Install 53
- Automated Installation using vApp properties and VMware OVF Tool 53
  - Manual Installation Using vApp Options 54
  - Touchless Installation Using VM Builder and VMware OVF Tools 55
- Install with Data Import 56
- Add a New Node to an Existing Cluster 57

---

**CHAPTER 5**

**Postinstallation Tasks 61**

- Postinstall Tasks for Cisco Unified Communications Manager 61

Reset Application User Passwords	63
Install the Real-Time Monitoring Tool	63
Enable the Kerneldump Utility	65
Install Licenses	66
Configure the Backup	66
Locale Installation	66
Install New Locales	67
Error Messages	68
COP File Installation Guidelines	69
Install a COP File	70
Install a Prebuilt Dial Plan	70
Restart the Cisco CallManager Service	71
Activate Security	71
Configure the Simple Network Management Protocol	72
Change Virtual Machine Configuration Specifications	72
Postinstall tasks for the IM and Presence Service	73
Activate services	74
Where to Go Next	74

---

**CHAPTER 6****Troubleshooting 75**

Network Errors During Installation	75
Failed Installations	76
Unrecoverable IM and Presence Service Node	76





# CHAPTER 1

## New and Changed Information

- [New and Changed Information](#), on page 1

### New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

**Table 1: New Features and Changed Behavior in Unified Communications Manager and IM and Presence Service**

Feature or Change	Description	See	Date
Initial Release of Document for Release 14SU2	—	—	June 16, 2022
Cluster Software Location	Unified Communications Manager now makes it easier to specify where cluster nodes will find their ISO files for upgrade or COP files, using the Cluster Software Location menu from the Cisco Unified OS Administration user interface.	<a href="#">Postinstall Tasks for Cisco Unified Communications Manager</a> , on page 61	June 16, 2022







## CHAPTER 2

# Planning the Installation

---

- [Topology Options, on page 3](#)
- [Installation Methods, on page 5](#)
- [Requirements and Limitations, on page 10](#)
- [Licensing Requirements, on page 16](#)
- [Required Installation Information, on page 19](#)
- [Export Restricted and Export Unrestricted Software, on page 24](#)

## 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 more information on scalability, see [Megacluster](#).

## 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 Centralized Cluster Deployment.

IM and Presence Deployment	Description
Standard Deployment (de-centralized/distributed )	<p>The IM and Presence Service cluster nodes are installed on the physical 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 Unified CM telephony clusters to IM and Presence clusters.</p> <p>Basic installations order followed is same as mentioned in the Attended Install method. For more information, see the "Installation Methods".</p> <p>For touchless installations, you can install all Unified Communications Manager and IM and Presence Service cluster nodes concurrently in a single process.</p>

IM and Presence Deployment	Description
IM and Presence Centralized Cluster Deployment	<p>The IM and Presence Service central cluster is installed separately from your telephony cluster and may be located on 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.</p> <p>For basic installations:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Install the IM and Presence Service database publisher node.</li> <li>3. Install any IM and Presence subscriber nodes.</li> </ol> <p>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.</p> <p>For more information, see the "Configure Centralized Deployment" chapter at <a href="#">Configuration and Administration of the IM and Presence Service Guide</a>.</p>

## Installation Methods

This guide covers the installation methods for Unified Communications Manager and IM and Presence Service.

These installation methods can be used for any of the following scenarios:

- Fresh Install (first-time setup of a brand-new node or cluster, no existing deployment, and no existing customer data).
- Expand a cluster (add a new subscriber node to an existing cluster).
- Direct Migration from an older version. For more information, see the [Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service](#).

Installation Method	Description
Attended Install	<p>A baseline-typical installation of one node of either Unified Communications Manager or IM and Presence Service, using the native Install Wizard graphical user interface (GUI). Unified Communications Manager only includes an option <b>Apply a Patch During an Upgrade</b> (for example, to apply a Service Update to the base release you are installing).</p> <p>To install a cluster using this method, follow the <a href="#">Attended Installation, on page 37</a> steps in this sequence:</p> <ul style="list-style-type: none"> <li>• Unified Communications Manager publisher node</li> <li>• Unified Communications Manager subscriber nodes</li> <li>• IM and Presence Service publisher node</li> <li>• IM and Presence Service subscriber nodes</li> </ul> <p>You can use this method with any of the following software media options:</p> <ul style="list-style-type: none"> <li>• Physical install DVD.</li> <li>• Bootable installer image for base release in ISO format (obtained from either Cisco Commerce Workspace, My Cisco Entitlements, or a Cisco Business Edition appliance factory preload).</li> <li>• Deployed OVA containing preinstalled application. This OVA format file contains fully installed, ready-to-run application, obtained from a Cisco Business Edition appliance factory preload.</li> <li>• Partial skip-installed OVA. This OVA format file contains partially installed application up to the "skip" Install Wizard point where the application is ready to accept an Answer File and complete installation. OVA format file is obtained either from My Cisco Entitlements or from a Cisco Business Edition appliance factory preload.</li> </ul> <p><b>Note</b> Use this method when manual installation without automation is acceptable, such as labs or small deployments.</p>

Installation Method	Description
<p>Touchless Install of a Single Node or a Cluster</p>	<p>A partially automated installation of one node or installation of clusterwide install of multiple nodes of Unified Communications Manager and IM and Presence Server.</p> <p>Use this method to get basic automation for one node, where you can fill out all the information initially, start the Install Wizard with that information, and complete the rest of the installation automatically using the Answer File.</p> <p>For clusterwide installations, use this method to generate pre-created Answer Files, that occurs in one seamless process with minimal intervention.</p> <p>To install a single node or a cluster using this method, follow the <a href="#">Touchless Installation Task Flow</a> steps:</p> <ol style="list-style-type: none"> <li>1. Create an Answer File for each node or node in the cluster using the Unified Communications Answer File Generator.</li> <li>2. Place all those Answer Files in well-known locations. See <a href="#">Generate Answer Files for Touchless Install</a>, on page 50.</li> <li>3. Power on the node or all the cluster nodes simultaneously.</li> </ol> <p>In this method, no interaction with the native Install Wizard is required. The nodes will communicate with each other and each node will read its Answer File for instructions.</p> <p>You can use this method with any of the software media options available for Attended Install. Use this method to:</p> <ul style="list-style-type: none"> <li>• Get more automation—Unattended Install of the entire cluster + zero interaction with the native Install Wizard.</li> <li>• Faster installation—Cluster nodes undergo installation in parallel. This is especially useful if you have a large cluster with many nodes to install.</li> </ul>

Installation Method	Description
Cisco Prime Collaboration Deployment (PCD)	<p>Fresh install, add nodes to, or direct migrate a cluster of Unified Communications Manager and IM and Presence Server using Cisco Prime Collaboration Deployment. See the <i>Cisco Prime Collaboration Deployment Administration Guide</i> for the following:</p> <ul style="list-style-type: none"> <li>• Fresh Install Task (where PCD performs similar operation as Touchless Install of a Single Node or Cluster).</li> <li>• Edit/Expand Task (where PCD performs similar operation as Touchless Install to add a single node).</li> <li>• Migration Task (where PCD is performing direct migration of an entire cluster).</li> </ul> <p>Use this method when:</p> <ul style="list-style-type: none"> <li>• You require assistance with multiple nodes of one cluster and/or multiple clusters, and a separate management application is acceptable.</li> <li>• (PCD Migration Task only) you are "repaving" an existing installation where you are dealing with one or more of the following: <ul style="list-style-type: none"> <li>• Two or more of these factors as part of the same migration—site moves, hardware changes, VMware upgrades, application version upgrades, application readdresses, and in scenarios where more flexibility is expected than what direct upgrades can provide.</li> <li>• You need to rebuild, restore or recover a cluster, or you need to revert configuration changes. Here, you are looking for a more flexible approach than what Unified Communications Manager Disaster Recovery Solution can provide.</li> <li>• It is acceptable to leverage application readdress and temporary extra hardware footprint to reduce migration downtime or duration.</li> </ul> </li> </ul>

Installation Method	Description
<p>VMware OVF Tool</p>	<p>Allows you to perform fully automated installation or direct migration of either a single node or an entire cluster, using the VMware OVF Tool.</p> <p>To install or direct migrate a cluster, follow the procedures at <a href="#">Automated Installation using vApp properties and VMware OVF Tool</a>, on page 53:</p> <ul style="list-style-type: none"> <li>• Use the VMware OVF Tool to create a skip-install OVA for each cluster node (with OVA parameters filled in, instead of using Answer File Generator).</li> <li>• Deploy all cluster nodes skip-installed OVAs simultaneously.</li> <li>• Installation continues like Touchless Install of a Single Node or Cluster or Fresh Install with Data Import.</li> </ul> <p>It is best to use this method with skip-install OVAs, as that provides the shortest duration and highest level of automation.</p> <p>Use this method when you require a programmatic install or direct migration method on top of any of the factors that drive consideration of Touchless Install of Cluster or Fresh Install with Data Import.</p>

Installation Method	Description
Fresh Install with Data Import	<p>Perform direct migration of either a single node or an entire cluster, using similar mechanisms as Prime Collaboration Deployment Migration task but native to Unified Communications Manager and IM and Presence.</p> <p>To directly migrate a cluster, follow the <a href="#">Install with Data Import</a> tasks:</p> <ul style="list-style-type: none"> <li>• On each cluster node, export your old version's data.</li> <li>• For each cluster node, provision a new virtual machine for your new version and follow either Attended Install or Touchless Install for a single node or the cluster node(s) of interest. Using the Data Import options available in Install Wizard and/or the Unified Communications Answer File Generator.</li> </ul> <p>You can use this method with any of the software media options available for Attended Install.</p> <p>Use this method for "native" direct migrations that don't require a separate management application like Prime Collaboration Deployment. You can have more granular control over individual nodes migration timing and sequencing. You may also use this method to avoid use of application readdress and temporary extra hardware footprint for direct migration.</p>
Node Installs	<p>If you want to add a node to an existing Unified Communications Manager or IM and Presence Service cluster for attended or touchless installation, complete the tasks in:</p> <p><a href="#">Add a New Node to an Existing Cluster, on page 57</a></p>

## 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.



### Note

- By default, your system is in non-FIPS mode, you must enable it, if desired.
- Ensure that the security password length is minimum 14 characters before you enable 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 14 requires minimum ESXi version of 6.7 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>.

---

## Subnet Limitations

Do not install Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. For more information, see [Cisco Collaboration System 12.x Solution Reference Network Designs \(SRND\)](#).

## 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, you 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 the IM and Presence Service Guide](#) for DNS configuration options.

## Firewall Requirements

Ensure that you configure your firewall so that connections to port 22 are open, and aren't throttled. During the installation of Unified Communications Manager and 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. For general security considerations, see the [Security Guide for Cisco Unified Communications Manager](#).




---

**Note** We recommend that you disable the "Intruder/Intrusion Detection" and/or "Brut Force Attack" features during upgrade and installs because these Firewall features are known to cause upgrades and installations to fail.

---

For more information on the port usage, see the chapter 'Cisco Unified Communications Manager TCP and UDP Port Usage' in the [System Configuration Guide for Cisco Unified Communications Manager](#).

## Platform Requirements

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.

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 14 requires minimum ESXi version of 6.7 U2 with minimum VM Hardware version of 13. For latest Unified Communications Manager ESXi version support, see [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/virtualization-cisco-unified-communications-manager.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html).

---

- deploy a virtual machine from the correct Cisco provided OVA file for the release. Depending on the installation method used, additional steps are required.

## Supported Versions

Unified Communications Manager and the IM and Presence Service nodes in the same cluster must be running the supported builds as mentioned in the [Release Notes for Cisco Unified Communications Manager and the IM and Presence Service](#).

### Version Mismatches

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

- Standard Deployments of IM and Presence Service—Both Unified Communications Manager and the IM and Presence Service must be running the supported versions for your deployment. A version mismatch is not supported.
- Centralized Deployments of IM and Presence Service—If you have the Centralized Deployment option configured on the IM and Presence Service, then within the IM and Presence Service central cluster, both the Unified Communications Manager instance and the IM and Presence Service must be running the same version. However, the telephony cluster that the central cluster connects to does not have to be running the same version.



---

**Note** The Centralized IM and Presence Service cluster requires a Unified CM publisher node, for a total of 7 servers in the cluster: 3 IM and Presence sub-cluster pairs (6 servers) + the Unified CM publisher node

---

## 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 provides and digitally signs. For more information, see the 'Operating System and Security Hardening' chapter in the [Security Guide for Cisco Unified Communications Manager](#).

You must perform all software installations and upgrades using Cisco Unified Communications Operating System Administration.

For information about software compatibility for Unified Communications Manager and IM and Presence Service, see the [Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service](#).

## Username and Password Requirements

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

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

### Administrator Account

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
- Cisco 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:

- Password must be at least 6 characters long and can contain alphanumeric characters, hyphens, and underscore.



---

**Note** If you plan to enable FIPS, Common Criteria, or Enhanced Security mode on any cluster, you must ensure that the security password is at least 14 characters long.

---

- Should not have the non-printable ASCII characters.
- Contains at least one alphanumeric character.
- 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 only alphanumeric characters.
- Do not use any non-alphanumeric characters.
- 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, abc123, qwerty, zyxwvuts, and 123321.
- 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.

## 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 Service 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.

## 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 before 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:



---

**Caution** 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 the "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](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 Service License Requirements

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




---

**Note** With the Jabber for Everyone offer, no end user licenses are required to enable IM and Presence Service 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 the [Administration Guide for Cisco Unified Communications Manager](#).
- The Bulk Administration Tool (BAT)
- Assign IM and Presence Service to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

For more information, see the [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 2: Required Installation Information**

Configuration Data	Description	Editable after Installation
<b>Administrator Credentials</b>		
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: <code>set password user admin</code>

Configuration Data	Description	Editable after Installation
<b>Application User Credentials</b>		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: <code>utils</code> <code>reset_application_ui_administrator_name</code>
Application User Password	Specifies the password for applications on the system.	Yes CLI: <code>utils</code> <code>reset_application_ui_administrator_password</code>
<b>Security Password</b>		
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: <code>set password user security</code>
<b>Certificate Information</b>		
Organization	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
Unit	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
Location	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
State	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>

Configuration Data	Description	Editable after Installation
Country	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state]</code>
<b>(Optional) SMTP</b>		
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 <b>Settings &gt; SMTP</b> and enter the IP address or Hostname in the SMTP Host Field.  • CLI: <code>set smtp [host]</code>
<b>NIC Interface Settings</b>		
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: <code>set network nic eth0 {auto   {en dis}} {speed  {10  100}} {duplex half  {half  full}}</code>  <b>Note</b> 1000BASE-T can only be enabled via auto-negotiation.  <b>Note</b> 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: <code>set network nic eth0 {auto   {en dis}} {speed  {10  100}} {duplex half  {half  full}}</code>  <b>Note</b> 1000BASE-T can only be enabled via auto-negotiation.  <b>Note</b> Virtual machines do not support this command.

Configuration Data	Description	Editable after Installation
<p>MTU Size</p> <p><b>Note</b> The MTU setting must be the same on all nodes in a cluster.</p>	<p>The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host transmits on the network.</p> <p>The value must not exceed the lowest MTU size that is configured on any link in your network.</p> <p>Default: 1500 bytes</p>	<p>Yes</p> <p>CLI: <code>set network mtu [size]</code></p>
<b>Network Information</b>		
<p>DHCP (Dynamic Host Configuration Protocol)</p>	<p>Select <b>Yes</b> if you want to use DHCP to automatically configure the network settings on your server.</p> <p>If you select <b>No</b>, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration.</p>	<p>Yes.</p> <ul style="list-style-type: none"> <li>In Cisco Unified Operating System Administration: select <b>Settings &gt; IP &gt; Ethernet</b>.</li> <li>CLI: <code>set network dhcp eth0 [enable]</code></li> <li>CLI: <code>set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]</code></li> </ul>
<p>Hostname</p>	<p>If DHCP is set to No, you must enter a hostname for this machine.</p>	<p>Yes; for Unified Communications Manager nodes, choose one of the following:</p> <ul style="list-style-type: none"> <li>In Cisco Unified Communications Operating System Administration, select <b>Settings &gt; IP &gt; Ethernet</b>.</li> <li>CLI: <code>set network hostname</code></li> </ul> <p>You will be prompted to enter the parameters.</p> <p>To change the hostname on Unified Communications Manager or IM and Presence server, see the 'IP Address, Hostname, and Domain Name Changes' section in the <a href="#">Administration Guide for Cisco Unified Communications Manager</a>.</p>

Configuration Data	Description	Editable after Installation
IP Address	If DHCP is set to No, you must enter the IP address of this machine.	<p>Yes; for Unified Communications Manager nodes, choose one of the following:</p> <ul style="list-style-type: none"> <li>In Cisco Unified Communications Operating System Administration, select <b>Settings &gt; IP &gt; Ethernet</b>.</li> <li>CLI: <code>set network IP eth0 [ip-address] [ip-mask]</code></li> </ul> <p>To change the IP address on Unified Communications Manager or IM and Presence server, see the 'IP Address, Hostname, and Domain Name Changes' section in the <a href="#">Administration Guide for Cisco Unified Communications Manager</a>.</p>
IP Mask	<p>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.</p> <p>The subnet mask must use the following format: 255.255.255.0</p>	<p>Yes</p> <ul style="list-style-type: none"> <li>In Cisco Unified Communications Operating System Administration, select <b>Settings &gt; IP &gt; Ethernet</b>.</li> <li>CLI: <code>set network IP eth0 [ip-address] [ip-mask]</code></li> </ul>
Gateway Address	If DHCP is set to No, you must enter the gateway address.	<p>Yes</p> <ul style="list-style-type: none"> <li>In Cisco Unified Communications Operating System Administration, select <b>Settings &gt; IP &gt; Ethernet</b>.</li> <li>CLI: <code>set network gateway [addr]</code></li> </ul>
<b>(Optional) DNS</b>		
DNS Primary	If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames.	<p>Yes</p> <p>CLI: <code>set network dns primary [address]</code></p>
DNS Secondary	When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server.	<p>Yes</p> <p>CLI: <code>set network dns secondary [address]</code></p>

Configuration Data	Description	Editable after Installation
Domain	Represents the name of the domain in which this machine is located	Yes CLI: <code>set network domain [name]</code>
<b>Timezone</b>		
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: <code>set timezone [zone]</code>
<b>Network Time Protocol</b>		
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. We recommend that you use the Unified Communications Manager publisher node as the NTP server.	Yes In Cisco Unified Communications Operating System Administration, select <b>Settings &gt; NTP Servers</b> .

## 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 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 of Unified Communications Manager and IM and Presence Service.

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

GUI Item	Location	Description
<b>SIP Federated Domains</b>	<b>Presence &gt; Inter-domain Federation &gt; SIP Federation</b>	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.
<b>XMPP Federation Settings</b>	<b>Presence &gt; Inter-domain Federation &gt; XMPP Federation &gt; Settings</b>	You cannot configure the security mode. It is set to <b>NO TLS</b> .
<b>Proxy Configuration Settings</b>	<b>Presence &gt; Routing &gt; Settings</b>	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.





# CHAPTER 3

## Preinstallation Tasks

- [Preinstall Tasks for Unified Communications Manager, on page 27](#)
- [Preinstall Tasks for the IM and Presence Service, on page 29](#)
- [Enable the Cisco AXL Web Service, on page 30](#)
- [Verify DNS Registration, on page 31](#)

## Preinstall Tasks for Unified Communications Manager

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Planning the Installation, on page 3</a>	Review the Planning chapter. Make sure to review the following: <ul style="list-style-type: none"> <li>• Decide on your installation method.</li> <li>• Decide on your cluster topology.</li> <li>• For IM and Presence Service, decide whether you are installing a standard deployment or an IM and Presence Service central cluster.</li> <li>• Review the Requirements and Limitations.</li> </ul>
<b>Step 2</b>	<a href="#">Required Installation Information, on page 19</a>	Review the installation requirements and record the configurations settings for each server that you plan to install.
<b>Step 3</b>	Create virtual machines.	<ul style="list-style-type: none"> <li>• Get base OVA.</li> <li>• Run the Collab Sizing Tool to get the required virtual machine count and specs of each virtual machine. If you don't want to run the Collab Sizing Tool, follow the guidance in the OVA readme and the OVA wizard to select a predefined</li> </ul>

	Command or Action	Purpose
		<p>starting point, which can be changed later if needed.</p> <ul style="list-style-type: none"> <li>If you are installing from a skip-install OVA from the factory preload of a Business Edition appliance, see <i>Installation Guide for Cisco Business Edition 6000 and 7000</i>.</li> </ul>
<b>Step 4</b>	Mount the installation ISO file.	<p>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.</p> <p>When you power on the virtual machine, it mounts the ISO file and start the installation process. Do not begin the installation process until you have completed all the steps in this procedure.</p>
<b>Step 5</b>	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 <a href="#">Cisco Unified Communications Solutions Reference Network Design</a> .
<b>Step 6</b>	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 Unified Communications Manager publisher node, run the <code>utils ntp status</code> CLI command.
<b>Step 7</b>	<p>Complete the following firewall updates:</p> <ul style="list-style-type: none"> <li>If a firewall is in the routing path between nodes, disable the firewall.</li> <li>Increase the firewall timeout settings until after you complete the installation.</li> </ul>	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.
<b>Step 8</b>	Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between servers where you are installing Unified Communications Manager.	
<b>Step 9</b>	Verify the NIC speed and duplex settings.	<p>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.</p> <p>For GigE (1000/FULL), you should set NIC and switch port settings to <code>Auto/Auto</code>; do not set hard values.</p>

	Command or Action	Purpose
<b>Step 10</b>	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].
<b>Step 11</b>	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 <a href="#">Verify DNS Registration, on page 31</a> .
<b>Step 12</b>	<a href="#">Licensing Requirements, on page 16</a>	Make sure that your system has adequate licensing.

## Preinstall Tasks for the IM and Presence Service

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Planning the Installation, on page 3</a>	Review the Planning chapter. Make sure to review the following: <ul style="list-style-type: none"> <li>• Decide on your installation method and cluster topology.</li> <li>• For IM and Presence Service, decide whether you are installing a standard deployment or an IM and Presence Service central cluster.</li> <li>• Review the Requirements and Limitations.</li> </ul>
<b>Step 2</b>	Supported Version	Make sure that the Unified Communications Manager and IM and Presence Service software versions are compatible.
<b>Step 3</b>	<a href="#">Required Installation Information, on page 19</a>	Gather all the information you need to complete the installation and configuration of the IM and Presence Service.
<b>Step 4</b>	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

	Command or Action	Purpose
		which you are deploying Unified Communications Manager. For more information, see <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html</a> .
<b>Step 5</b>	Verify network connectivity.	Make sure that each IM and Presence Service server has network access to the Unified Communications Manager publisher server. Ping the Unified Communications Manager publisher node from the other IM and Presence Service servers.
<b>Step 6</b>	<a href="#">Enable the Cisco AXL Web Service, on page 30</a>	Make sure that the Cisco AXL Web Service is enabled.
<b>Step 7</b>	<a href="#">Verify DNS Registration, on page 31</a>	<p>If you use DNS, ensure that you have configured the hostname of the new IM and Presence Service 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 Service servers (if any).</p> <p><b>Note</b> We recommend that you use the same DNS servers between IM and Presence Service 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 Service must either use DNS, or not use DNS, because it does not support mixed-mode deployments.</p>

## 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 4

## Installation Methods

- [Installation Methods Task Flows](#), on page 33
- [Attended Installation Task Flow](#), on page 35
- [Touchless Installation Task Flow](#), on page 49
- [Automated Installation using vApp properties and VMware OVF Tool](#), on page 53
- [Install with Data Import](#), on page 56
- [Add a New Node to an Existing Cluster](#), on page 57

## Installation Methods Task Flows

Choose one of the following installation methods task flows:

Task Flow	Description
<a href="#">Attended Installation Task Flow</a> , on page 35	Use this method for basic installs of any of the following deployments: <ul style="list-style-type: none"> <li>• Unified Communications Manager telephony cluster installs</li> <li>• Standard Deployments (Decentralized) for IM and Presence</li> </ul>
<a href="#">Touchless Installation Task Flow</a> , on page 49	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.
<a href="#">Automated Installation using vApp properties and VMware OVF Tool</a> , on page 53	Use this method to install a Unified Communications Manager or IM and Presence Service cluster using skip-install OVAs.
<a href="#">Install with Data Import</a> , on page 56	Complete this tasks to install a Unified Communications Manager or IM and Presence Service cluster using the <b>Install with Data Import</b> .
<a href="#">Add a New Node to an Existing Cluster</a> , on page 57	Complete these tasks if you want to add a node to an existing Unified Communications Manager or IM and Presence Service cluster.

## Installation Wizard Considerations

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 Service 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 Service 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.
- Note 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 Cluster Deployment or in a Standard Deployment (de-centralized/distributed).

### Installation Wizard

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

**Table 3: 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: \, - , \_ ; { } O [ ]

All other characters are not supported.

## Attended Installation Task Flow

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

- Installs of a Unified Communications Manager telephony cluster
- Installs of the IM and Presence Service in a Standard Deployment (de-centralized/distributed).



**Note** Depending on your installation scenario, you may not need to perform all 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

[Preinstall Tasks for Unified Communications Manager, on page 27](#)

[Preinstall Tasks for the IM and Presence Service, on page 29](#)

	Unified Communications Manager	IM and Presence Service	Description
Step 1	<a href="#">Attended Installation, on page 37</a>	—	Begin the install process for Unified Communications Manager.
Step 3	(Optional) Complete either of the following tasks: <ul style="list-style-type: none"> <li>• <a href="#">Upgrade Install Image from Local Source, on page 39</a></li> <li>• <a href="#">Upgrade Install Image from Remote Server, on page 40</a></li> </ul>	—	Upgrade your install image to a newer version. This optional task is available for Unified Communications Manager installs only.

	Unified Communications Manager	IM and Presence Service	Description
Step 4	<a href="#">Configure Attended Installation, on page 42</a>	—	Continue with the Attended Installation process by configuring your installation.
Step 5	<a href="#">Configure the Unified Communications Manager Publisher, on page 44</a>	—	Configure and install software on the publisher node.
Step 6	<a href="#">Add Subscriber Nodes, on page 47</a>	—	Add subscriber nodes to the publisher node.
Step 7	<a href="#">Install Subscriber Nodes, on page 48</a>	—	Install software on your Unified Communications Manager subscriber nodes.
Step 8	—	<a href="#">Attended Installation, on page 37</a>	Begin the install process for the IM and Presence Service.
Step 10	—	<a href="#">Configure Attended Installation, on page 42</a>	Continue Attended Install process for IM and Presence Service by configuring the installation.
Step 11	—	<a href="#">Configure the IM and Presence Publisher, on page 47</a>	Configure and complete the installation for the IM and Presence Service database publisher node.
Step 12	<a href="#">Add Subscriber Nodes, on page 47</a>	—	On the Unified Communications Manager publisher node, add the IM and Presence Service subscribers.
Step 13	—	<a href="#">Install Subscriber Nodes, on page 48</a>	Install software on your IM and Presence Service subscriber nodes.

## Install IM and Presence Central Cluster (Attended Installation)

Complete these tasks to install an IM and Presence Service Centralized Deployment using basic attended 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 Service Central Cluster



**Note** For basic installation of IM and Presence Service in a de-centralized/distributed (Standard) deployment, follow the [Installation Methods Task Flows, on page 33](#) to install both the telephony and IM and Presence Service clusters.

	Unified CM Publisher (non-telephony)	IM and Presence Service Central Cluster	Description
Step 1	<a href="#">Attended Installation, on page 37</a>	—	Begin the install process for the Unified CM publisher node.
Step 2	<a href="#">Configure Attended Installation, on page 42</a>	—	Configure the Basic Installation.
Step 3	<a href="#">Configure the Unified Communications Manager Publisher, on page 44</a>	—	Configure the Unified CM publisher node.
Step 4	—	<a href="#">Attended Installation, on page 37</a>	Begin the install process for the IM and Presence central cluster.
Step 5	—	<a href="#">Configure Attended Installation, on page 42</a>	Continue with the Basic Install process for IM and Presence Service by continuing the installation.
Step 6	—	<a href="#">Configure the IM and Presence Publisher, on page 47</a>	Configure the IM and Presence Service database publisher node.
Step 7	<a href="#">Add Subscriber Nodes, on page 47</a>	—	On the Unified CM publisher, add IM and Presence Service subscriber nodes.
Step 8	—	<a href="#">Install Subscriber Nodes, on page 48</a>	Complete the installation on the IM and Presence Service subscribers.

## Attended 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** 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.

**Note** If you are installing Unified CM or IM and Presence Service from a Cisco Business Edition 6000/7000 appliance with the software pre-installed, go directly to the [Installation Guide for Cisco Business Edition 6000 and 7000](#) for more information.

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

**Step 2** Click **Yes** to perform the media check. Or click **No** to skip the media check.

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

**Step 3** 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](http://cisco.com) or obtain another DVD or ISO directly from Cisco.

**Step 4** 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**.

**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 5** If the Unified CM or IM and Presence Service software is pre-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 6** 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.
- To continue with **Install with Data Import**, choose **Proceed**.

Allows you to configure Unified Communications Manager and Instant Messaging and Presence Service installation with Data Import.

- 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 7** In the **Apply Additional Release** window, if you have a newer Unified Communications Manager SU version on the same major release 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 39](#)
- [Upgrade Install Image from Remote Server, on page 40](#)
- **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 8** In the **Basic Install** window, click **Continue** to install the software or configure the pre-installed software.

---

### What to do next

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

- [Upgrade Install Image from Local Source, on page 39](#)
- [Upgrade Install Image from Remote Server, on page 40](#)

To continue the basic install process, [Configure Attended Installation, on page 42](#).

## 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, see [Upgrade Install Image from Remote Server, on page 40](#).

---

### Before you begin

Make sure to do the following:



---

**Note** To complete this procedure, you must have completed the [Attended Installation, on page 37](#) procedure and have chosen to apply a patch via a LOCAL source.

---

- Start a basic installation. Choose the option to apply a patch via a LOCAL source. For details, see [Attended Installation, on page 37](#).
- 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

[Configure Attended Installation, on page 42](#)

## 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, see [Upgrade Install Image from Local Source, on page 39](#).

---

### 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 and then continue.
- Note** To use this option, your hub or the 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 transmits 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 Attended Installation, on page 42](#) procedure to configure the basic installation.
- 

### What to do next

[Configure Attended Installation, on page 42](#)

## Configure Attended Installation

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

### Before you begin

[Attended Installation, on page 37](#)

### 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** contains alphanumeric characters. Use the same login credentials 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, on page 44](#)
- [Configure the IM and Presence Publisher, on page 47](#)

Otherwise, for subscriber node installs [Add Subscriber Nodes, on page 47](#).

## 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 attended installation and configured the attended installation.



---

**Note** You can configure Smart Call Home on the publisher node only.

---

### Procedure

---

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

We recommend 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 we recommend 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](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.

**Note** If you choose **Install with Data Import** during basic installation the **Application User Configuration** window does not appear. Proceed to step 11 to complete the installation.

**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 47](#).

## 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 47](#)

## 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 Service 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 Service 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 Service nodes.
- 

### What to do next

Install Subscriber Nodes

## 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, [Add Subscriber Nodes, on page 47](#).

### 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 [Attended Installation, on page 37](#) 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 61](#)
- [Postinstall tasks for the IM and Presence Service, on page 73](#)

## Touchless Installation Task Flow

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

### Before you begin

[Preinstall Tasks for Unified Communications Manager, on page 27](#)

[Preinstall Tasks for the IM and Presence Service, on page 29](#)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Generate Answer Files for Touchless Install, on page 50</a>	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 a single node or the various cluster nodes.

	Command or Action	Purpose
<b>Step 2</b>	<a href="#">Generate Virtual Floppy Images, on page 51</a>	Use this procedure to create virtual floppy images from the answer files. You use the virtual floppy images in your touchless installation.
<b>Step 3</b>	<a href="#">Upload Virtual Floppy Image to Datastore, on page 52</a>	Use this procedure to upload the virtual floppy images to the datastore.
<b>Step 4</b>	<a href="#">Mount Floppy Image to VM, on page 52</a>	Use this procedure to mount the UC application virtual floppy images on their corresponding VM.
<b>Step 5</b>	<a href="#">Run Touchless Install, on page 53</a>	Begin the single node or 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** In the **Software Location of Data to Import** section, check the **Configure Software Location of Data to Import** check box to configure Remote SFTP server details only if you choose to install using the Fresh Install with Data Import. Else ignore this step and proceed to step 5. For more details, see [Install with Data Import, on page 56](#).

By checking the **Configure Software Location of Data to Import** 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 fields:

- **Remote Server Name or IP**—The Secure FTP (SFTP) server that stores the source cluster's exported data.
- **Export Data Directory**—Directory path of the server containing export data.
- **Remote Server Login ID**—Allows data retrieval of the remote SFTP server.



- **Remote Server Password**—Can contain alphanumeric characters, hyphens, and underscores.

- Step 5** Complete the remaining fields under **Clusterwide Configuration** with your cluster configuration details.
- Step 6** Complete the fields in the **Primary Node Configuration** with configuration details for the publisher node.
- Step 7** 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 8** Under **Secondary Node Configuration**, enter the node details for your first subscriber node and click **Add Secondary Node**.
- Step 9** Add all your subscriber nodes.
- Step 10** Add all your cluster nodes and click **Generate Answer files**.
- Step 11** Download the answer files to your computer.
- Step 12** Repeat this procedure to generate answer files for the IM and Presence Service cluster.

---

#### What to do next

[Generate Virtual Floppy Images, on page 51](#)

## 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, on page 52](#)

## 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 your local 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, on page 52](#)

## 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, on page 53](#)

## 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:
- CD-Rom
  - Hard Drive
  - Removable Devices
  - Network
- Step 4** Save the settings and exit from the console. The installation commences immediately.
- Step 5** Repeat these steps for each cluster node. All cluster nodes may install in parallel; you do not have to install them serially.
- Step 6** After to emphasise the completion of an activity, remove the vFloppy configurations from the virtual machines.
- 

**What to do next**

[Postinstall Tasks for Cisco Unified Communications Manager, on page 61](#)

[Postinstall tasks for the IM and Presence Service, on page 73](#)

## Automated Installation using vApp properties and VMware OVF Tool

This feature uses a skip-install Open Virtual Archive (OVA) file containing an application that is installed up to the “skip” configuration point, where the application is ready to accept the configuration and complete installation. The VMware OVF Tool is used to deploy and inject the Unified CM and IM and Presence Service configuration parameters into the virtual machines using skip-install OVA and vApp properties without using Answer File Generator or vFloppy images.

Deployment vApp options are available for virtual machines that are deployed from VMware Open Virtualization Format Tool (OVF) Tool to the desktop or to the web server (Application available only on vcenter). For a virtual machine with vApp options enabled, the vApp options are preserved when you export the virtual machine as an OVF template. Without manual intervention from the administrators, you just need the skip-install OVA image to install the entire Unified CM clusters. Using the vApp parameters, you simply need to define a template and set the values of vApp Properties and inject all the details during deployment of the skip-install OVA using the VMware OVF Tool that results in automated installation.

Fresh Install and Fresh Install with Data Import is supported using this method. You can deploy this installation in two ways:

- **Manual Installation Using vApp Options**—Deploy the skip-install OVA on each node in the cluster manually by logging into the respective VMware Embedded Host Client or vCenter Server, where the Unified CM server configurations can be entered.
- **Touchless Installation Using VM Builder and VMware OVF Tools**—Run the VM Builder tool (which is a VMware wrapper tool that is provided as part of the platform skip-install-ova rpm/tar) by passing the Unified CM configuration parameters, skip-install OVA, and VMware Embedded Host Client or vCenter Server details of each node in the cluster, which would perform the complete cluster installation without manual intervention.

## Manual Installation Using vApp Options

This option allows you to deploy OVA manually in the VMware Embedded Host Client or vCenter Server where OVA needs to be placed either in the desktop or to the web server.




---

**Note** The OVA deployment from a web server is applicable only for vCenter.

---




---

**Note** While deploying skip-install OVA through vCenter, you will see additional terminologies in the **First Node Access Configuration (Set ONLY on SUBSCRIBERS)** field in the customization template. For example, *First Node Access Configuration (Set ONLY on 2 settings SUBSCRIBERS)*. We recommend that you ignore the term **2 settings** in this field as this term is parsed from the vCenter configuration settings.

---




---

**Note** This task is only supported with VMware Embedded Host Client or vCenter Server versions 6.7 and 7.0.

---

### Procedure

---

- Step 1** Deploy skip-install OVA after obtaining it from **My Cisco Entitlements**.
- Step 2** From VMware Embedded Host Client or vCenter Server, deploy OVA from the desktop using the **Browse** button or enter a URL to download and install the OVA package from the Internet.
- Step 3** If the OVA is placed in a web server, enter the respective URL while deploying the OVA. For example, *http://10.xx.xx.xx/UCSInstall\_UCOS\_14.xxx.ova*.
- Step 4** Enter the required Unified CM configurations, skip-install OVA, VMware Embedded Host Client, or vCenter for each node in the cluster.

The configuration is different for publisher and subscriber nodes. See the Required Installation Information help page to fill the mandatory configuration details.

**Note** With this installation method, you can add up to 5 Unified Communication Manager subscriber nodes and 5 IM and Presence Service nodes in the user interface of Unified CM publisher. If we need to add more subscribers (Unified CM or IM and Presence Service), follow step 5 or step 6 depending on the deployment.

**Step 5** To perform touchless install on entire cluster including publisher, make sure to check the **Dynamic Cluster Config Enable** check box in user interface of the Unified Communication Manager publisher, and enter a value between 1-24 in the Dynamic cluster Config Timer field.

**Step 6** To install subscriber nodes in the cluster after the Unified CM publisher installation completes, perform any one of the following:

- Enable the Dynamic Cluster Config Timer option in Unified Communication Manager publisher using the CLI **set network cluster subscriber dynamic-cluster-configuration no-of-hours|default**. (OR)
- Add your subscriber nodes manually from the user interface of the Unified CM publisher, after the Unified CM publisher node installation completes.

**Step 7** For installation using Fresh Install with Data Import, follow the instructions as described in [Attended Installation Task Flow, on page 35](#) from step 1 through 6 to export data from source node. See [Install with Data Import, on page 56](#).

**Step 8** Once the OVA image is deployed successfully into the virtual machine, power on the Virtual Machine.

You will observe that the installation is in process. Repeat step 4 for each subscriber node in the cluster by providing the **IP Address** and **Host Name** of the Unified CM publisher nodes. Subscriber nodes can be installed parallelly by opening multiple VMware Embedded Host Clients.

**Note** If DHCP is enabled for OVA deployment, ensure that you go to the edit settings of the virtual machine and change the **MAC** option to manual (by default, this option is automatic) before powering-on the virtual machine. Enter the static MAC address mapped with the **IP Address** and **Host Name** for the Unified Communications Manager and IM and Presence Service nodes.

---

## Touchless Installation Using VM Builder and VMware OVF Tools

This task allows to deploy skip-install OVA using the Cisco VM Builder tool, which is a wrapper tool to inject the configurations parameters.



---

**Note** This task is only supported with VMware Embedded Host Client or vCenter Server versions 6.7 and 7.0.

---

### Before you begin

- Requires a Linux server to run Cisco VM Builder and VMware OVF Tool.

The Cisco VM Builder tool (VMware wrapper tool) and the dependent tool will be bundled and provided as .rpm file (platform-skip-install-ovftool-1.0.0.0-1.x86\_64.rpm) or as a g-zipped tar file/tarball (platform-skip-install-ovftool\_v1.0.tar.gz.) See the ReadMe guide for instructions on how to install .rpm/tar.

## Procedure

---

- Step 1** Install the Cisco VM Builder tool on any Linux server. It can be an SFTP server as well.
- Step 2** Copy the Unified Communications Manager and IM and Presence Service OVA image to the same server.
- Step 3** Using the Cisco VM Builder tool, pass the required Unified CM configurations, skip-install OVA, and VMware Embedded Host Client or vCenter for each node in the cluster based on the type of Install. Install can be Fresh Install or Fresh Install with Data Import.

Configurations differ for the publisher and subscriber nodes. Use the “vmbuilder--help” option to know more about the parameters to be used.

**Note** With this installation method, you can add up to 5 Unified Communication Manager subscriber nodes and 5 IM and Presence Service subscriber nodes in the Cisco VM Builder tool of the Unified CM publisher. If we need to add more subscribers (Unified CM or IM and Presence Service), follow step 4 or step 5 depending on the deployment.

- Step 4** To perform touchless install on entire cluster including publisher, make sure to pass the **Dynamic Cluster Config Enable** parameter as **True** and enter a value between 1-24, in the Dynamic cluster Config Timer in the Cisco VM Builder tool of the Unified CM publisher. For example, set the values of these parameters as: **guest.dynamic\_cluster\_config=True** and **guest.cluster\_config\_timer=24**.
- Step 5** To install subscriber nodes in the cluster after the Unified CM publisher installation completes, perform any one of the following:
- Enable the **Dynamic Cluster Config Enable** option in the user interface of the Unified Communication Manager publisher using the CLI **set network cluster subscriber dynamic-cluster-configuration no-of-hours|default**. (OR)
  - Add your subscriber nodes manually from the Unified CM user interface of the publisher, after the Unified CM publisher node installation completes.
- Step 6** The Cisco VM Builder tool validates the configuration values, deploys the OVA in the VMware Embedded Host Client or vCenter Server, automatically powers on the node, and starts the installation.
- See the “vmbuilder--help” option to know more about the mandatory parameters and other restrictions.
- Step 7** Repeat step 3 for each subscriber node in the cluster. Subscriber nodes can be installed parallelly by opening multiple SSH connections.
- Note** DHCP is not supported for touchless installation as the automated MAC can assign any **IP Address** and **Host Name** for the nodes.
- 

## Install with Data Import

Use one of these steps to configure Unified Communications Manager and IM and Presence Service installation with data import from an older version of Unified CM.



---

**Important** You must not change the configuration settings on any Publisher or Subscriber node until Data export is completed on all the nodes in the cluster. If there are any configurations changes required, ensure that you Export data on all the nodes again.

---

See the [Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service](#) to refer to the supported source releases for direct migration to the 14SU2 destination versions.

### Before you begin

Run the **utils system upgrade dataexport initiate** CLI command on each node of the desired source system to export the data which can be imported using this procedure. Your source version must be Release 10.5 or higher. If your source version is not Release 12.5(1) SU5 or higher, you must install the latest version of the "ciscocm.DataExport" COP file on each node of the source system.

### Procedure

---

- Step 1** To configure Unified Communications Manager and IM and Presence Service with **Install with Data Import** follow the instructions as described in [Attended Installation, on page 37](#) from steps 1 through 6. Then proceed with the following steps:
- In the **Platform Installation Wizard** window, click **Import** to import data from the SFTP server during the Unified Communications Manager and IM and Presence Service installation. The installation process starts with preinstallation and nodes are rebooted.
  - After reboot, click **OK** in **Import Upgrade Configuration Information** screen.  
To continue the basic install process, see [Configure Attended Installation, on page 42](#).
- Step 2** To configure Unified Communications Manager and IM and Presence Service with **Install with Data Import** follow the instructions as described in [Touchless Installation Task Flow, on page 49](#) from steps 1 through 5.
- Step 3** To configure Unified Communications Manager and IM and Presence Service with **Install with Data Import** follow the instructions as described in [Touchless Installation Using VM Builder and VMware OVF Tools, on page 55](#) from steps 1 through 7.
- 

## 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 attended Installation or Installation Using VM Builder and VMware OVF Tools methods to add and install the node. Any new nodes that you add must be configured as subscriber nodes.

### Attended Installation

For attended 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 <a href="#">Administration Guide for Cisco Unified Communications Manager</a> .
Step 2	<a href="#">Attended Installation, on page 37</a>	Begin the installation process.
Step 3	<a href="#">Configure Attended Installation, on page 42</a>	Continue with the Attended Installation process by configuring your installation.
Step 4	<a href="#">Add Subscriber Nodes, on page 47</a>	Add subscriber nodes to Unified Communications Manager publisher.
Step 5	<a href="#">Install Subscriber Nodes, on page 48</a>	Install software on your subscriber nodes.

### Touchless Installation

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

	Procedure	Description
Step 1	Run a full backup of the cluster.	For details, see the "Manage Backups" chapter of the <a href="#">Administration Guide for Cisco Unified Communications Manager</a> .
Step 2	<a href="#">Generate Answer Files for Touchless Install, on page 50</a>	Generate answer files for your installation. The touchless install process uses answer files to install and configure the various cluster nodes.
Step 3	<a href="#">Generate Virtual Floppy Images, on page 51</a>	Create a virtual floppy image from the answer file.
Step 4	<a href="#">Upload Virtual Floppy Image to Datastore, on page 52</a>	Upload the virtual floppy to the datastore.
Step 5	<a href="#">Mount Floppy Image to VM, on page 52</a>	Mount the virtual floppy to the virtual machine.
Step 6	<a href="#">Run Touchless Install, on page 53</a>	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 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 simultaneously install multiple Unified Communications Manager and multiple IM and Presence Service nodes. The following scenarios are supported:

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

If you need to simultaneously 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.





## CHAPTER 5

# Postinstallation Tasks

- [Postinstall Tasks for Cisco Unified Communications Manager](#), on page 61
- [Postinstall tasks for the IM and Presence Service](#), on page 73
- [Where to Go Next](#), on page 74

## Postinstall Tasks for Cisco Unified Communications Manager

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	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.  <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html</a>
<b>Step 2</b>	Configure Software Location on cluster nodes that will be used for future upgrades and COP Installs.	Before you attempt to upgrade any cluster nodes or install any COP files on the cluster nodes, all cluster nodes need to have their Software Location fields configured. For more information on configuring software location details, see the 'Configure Cluster Software Location' section in the <a href="#">Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service</a> from Releases 12.5(1)SU6 and 14SU2 onwards.
<b>Step 3</b>	<a href="#">Reset Application User Passwords</a> , on page 63	We recommend that you reset your application user passwords post installation.
<b>Step 4</b>	<a href="#">Install the Real-Time Monitoring Tool</a> , on page 63	You can use the Cisco Unified Real-Time Monitoring Tool (RTMT) to monitor Unified

	Command or Action	Purpose
		Communications Manager and the IM and Presence Service in real time.
<b>Step 5</b>	<a href="#">Enable the Kerneldump Utility, on page 65</a>	If you have a kernel crash, the kerneldump utility provides a mechanism for collecting and dumping the crash.
<b>Step 6</b>	<a href="#">Install Licenses, on page 66</a>	Verify that you have the required licenses for your system and devices.
<b>Step 7</b>	<a href="#">Configure the Backup, on page 66</a>	We recommend performing regular backups. You can set up automatic backups or invoke a backup at any time.
<b>Step 8</b>	<a href="#">Install New Locales, on page 67</a>	Optional. The default locale is US - English. If you want to use a different locale, download and install it.
<b>Step 9</b>	<a href="#">COP File Installation Guidelines, on page 69</a>	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.
<b>Step 10</b>	Install a dial plan by completing these tasks: <ul style="list-style-type: none"> <li>• <a href="#">Install a COP File, on page 70</a></li> <li>• <a href="#">Install a Prebuilt Dial Plan, on page 70</a></li> <li>• <a href="#">Restart the Cisco CallManager Service, on page 71</a></li> </ul>	If you want to use a dial plan other than the North American Numbering Plan (the default), you must download and install it.
<b>Step 11</b>	<a href="#">Activate Security, on page 71</a>	Optional. If you want to enable security on your system, install the Cisco CTL Client and enable mixed mode.
<b>Step 12</b>	<a href="#">Configure the Simple Network Management Protocol, on page 72</a>	Optional. If you are using a Network Management System such as Cisco Prime Collaboration Assurance, enable the Simple Network Management Protocol.
<b>Step 13</b>	<a href="#">Change Virtual Machine Configuration Specifications, on page 72</a>	To change to the Guest OS version in the Cisco Unified Communications Manager virtual machine (VM) settings.
<b>Step 14</b>	Ensure that you configure the <b>Trusted List of Hosts in HTTP Referer/Host Header</b> and add the public IP address or DNS alias in the Cisco Unified CM Administration Enterprise Parameters page.	This configuration is necessary if your network topology has public IP address configured for external interfaces along with private IP address for the individual nodes in the cluster. Unified CM will now validate the IP address or hostname present in the Host header with the servers configured in the Unified CM cluster first before allowing access to Unified

	Command or Action	Purpose
		<p>CM. You must also configure the DNS alias used to access the Unified CM under the Trusted List of Hosts configuration. For example, if your server is <code>cm1.example.local</code>, and you use <code>phone.example.local</code> to access the server, you must add <code>phone.example.local</code> to the Trusted List of Hosts configuration.</p> <p>From the private network using a private IP address, navigate to the Cisco Unified CM Administration user interface and select <b>System &gt; Enterprise Parameters</b> to configure the external IP addresses or DNS alias used.</p> <p>You must restart the Cisco Tomcat service after performing this activity for all the web pages to load correctly.</p>

## Reset Application User Passwords

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

### Procedure

- 
- Step 1** From Cisco Unified CM Administration, choose **User Management > Application User**.
  - Step 2** Click **Find**.
  - Step 3** Click 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 <b>Application &gt; Plugins</b> .
Unified Communications Manager IM and Presence Service	From Unified Communications Manager IM and Presence Administration, choose <b>Application &gt; Plugins</b> .
Cisco Unity Connection	From Cisco Unity Connection Administration, choose <b>System Settings &gt; Plugins</b> .

### 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 kerneldump 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

We recommend 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](#).

## 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](http://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 your upgrades and migrations. For upgrades, you must reinstall any locales that you are using, except for 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. We strongly recommend 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](https://www.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.

Message	Description
[LOCALE] Communications Manager CSV file installer installldb is not present or not executable.	This error occurs because a Unified Communications Manager application called installldb 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_<II>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<II>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<II>_<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/LocaleMasterVersion.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.
[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 70](#).

## 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 70](#).

### 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 71](#)

## 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, see the [Security Guide for Cisco Unified Communications Manager](#).

## 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, configure the SNMP user.
  - Step 6** Configure the notification destination for traps or informs.
  - Step 7** Configure the system contact and location for the MIB2 system group.
  - Step 8** Configure trap settings for CISCO-SYSLOG-MIB.
  - Step 9** Unified Communications Manager only: Configure trap settings for CISCO-CCM-MIB.
  - Step 10** Restart the Primary Agent service.
  - Step 11** 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 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 status** and click **Upgrade** to match host.
- b. Update Guest OS—Right click the **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 [Configuration and Administration of the IM and Presence Service Guide](#). Where indicated, see that guide for detail on how to complete these tasks.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	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.  <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html</a>
<b>Step 2</b>	Check for software and firmware updates for IM and Presence Service on Cisco.com.	You can download software from <a href="https://software.cisco.com/download/navigator.html?mdfid=280448682&amp;i=rm">https://software.cisco.com/download/navigator.html?mdfid=280448682&amp;i=rm</a>
<b>Step 3</b>	Configure Presence Redundancy Groups.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .

	Command or Action	Purpose
<b>Step 4</b>	Change the default domain.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 5</b>	Change the IM and Presence Service IM address scheme.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 6</b>	Change the IM and Presence Service node name.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 7</b>	Configure Unified Communications Manager as a Presence Gateway.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 8</b>	Configure a SIP Publish trunk on Unified Communications Manager.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 9</b>	Assign users to servers.	For details, see the <a href="#">Configuration and Administration of the IM and Presence Service Guide</a> .
<b>Step 10</b>	<a href="#">Activate services, on page 74</a>	Turn on essential IM and Presence Service 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. See the following guide for details on how to configure your system:

- [System Configuration Guide for Cisco Unified Communications Manager](#)





## CHAPTER 6

# Troubleshooting

- [Network Errors During Installation, on page 75](#)
- [Failed Installations, on page 76](#)
- [Unrecoverable IM and Presence Service Node, on page 76](#)

## 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. Sometimes, 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.

### Steps to Recover Logs using Recovery CD

You should use the Recovery CD to recover the logs to access the diagnostic information. Follow the steps mentioned:

1. Insert the recovery CD.

2. Reboot the system.
3. Once the recovery CD menu comes up, press Alt + F2 to get to the command prompt.
4. Find the largest partition by performing a "df -h". (/mnt/part6).
5. Locate the install logs at: /mnt/part6/log/install/ directory.
6. Collect the logs.

## 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.