# CONTENTS

**Preface**
ix
- Purpose ix
- Audience ix
- Organization ix
- Related documentation x
- Conventions xi
- Obtain support xii
- Cisco product security overview xii

## Part I
Cisco Unified CM installation 1

## Chapter 1
Cisco Unified Communications Manager installation 3
- Installation scenarios 3
  - Install software from a DVD on the first node 4
  - Install software from a DVD on a subsequent node 4
  - Apply a patch during installation of the first node 5
  - Apply a patch during installation of a subsequent node 5
  - Add a new node to an existing cluster 6
  - Reuse the MCS-7828 7
  - Parallel installations of cluster nodes 8
- Pre-installation tasks 8
- Important considerations 9
- Frequently asked questions 11
  - Installation time 11
  - User name and password requirements 11
  - Password considerations 12
  - Server support 13
PART II

IM and Presence Service installation 41

CHAPTER 2

New in this release 43

Rebranding to IM and Presence 43
Version alignment 43
Centralized profile configuration and data migration 44
Licensing simplification 44
Deprecated features 44

CHAPTER 3

Product description 45

Overview of IM and Presence 45
Publisher and subscriber nodes 45
Interaction with Cisco Unified Communications Manager 46
System time on IM and Presence publisher node 46
IM and Presence license requirements 47

CHAPTER 4

Before you begin 49

Read this first 49
DNS requirements 49
Installation time requirements 50
System requirements 50
Required passwords 50
Administrator account username and password 50
Application username and password 50
Security password 51
Required installation information 51
Hardware and software requirements 58
Hardware requirements 58
Software restrictions 58
Perform pre-installation tasks 58
Cluster topology 59
Deploy multiple nodes in cluster 59
Unattended installation of IM and Presence 60
Generate answer file 60
CHAPTER 5

Installation

Installation overview

Installation and configuration taskflows

Run unattended installation and configuration of publisher node
Run unattended installation and configuration of subscriber node
Manually install and configure publisher node
Manually install and configure subscriber node
Add new node to existing cluster

Navigation of installation wizard

Installation and configuration of IM and Presence

Media check
Use answer file to install and configure IM and Presence
Start basic installation
Configure basic installation
Configure publisher node
Run post-installation deployment wizard
Configure subscriber node
Configure pre-installed IM and Presence server

Perform fresh multi-node installation

CHAPTER 6

Post-installation tasks

Perform post-installation tasks

Software and firmware updates
Apply latest Firmware upgrade
Check for software upgrades
Configure Cisco Unified Communications Manager as Presence Gateway
Configure SIP Trunk on Cisco Unified Communications Manager
User and server assignments
Activate services
Change of IM and Presence node name to resolvable value
Change of default Presence domain name

CHAPTER 7

Reference
RAID and BIOS settings 87
Access Cisco Unified CM IM and Presence Administration 88
Preface

- Purpose, page ix
- Audience, page ix
- Organization, page ix
- Related documentation, page x
- Conventions, page xi
- Obtain support, page xii
- Cisco product security overview, page xii

Purpose

This document describes how to install the following software:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service

Audience

This Installation Guide is intended for administrators who are responsible for installing Cisco Unified Communications Manager and IM and Presence Service software.

Organization

The following table shows how this guide is organized:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Part 1  | “Cisco Unified CM installation”  
|         | Provides instructions to install Unified CM Release 9.0(1). |
For additional installation and upgrade information, refer to the following documents:

- **Upgrading Cisco Unified Communications Manager**
  This document describes how to upgrade Cisco Unified Communications Manager from Release 6.1(2) and later.

- **Upgrade Guide for Cisco Unified Communications Manager**
  This document describes how to upgrade Cisco Unified Communications Manager to a later appliance-based release.

- **Cisco Unified Communications Operating System Administration Guide**
  This document provides information about upgrading the Cisco Unified Communications Manager to a later appliance-based release.

- **Replacing a Single Server or Cluster for Cisco Unified Communications Manager**
  This document describes how to replace a Cisco Unified Communications Manager server or a cluster of servers.

- **Command Line Interface Reference Guide for Cisco Unified Communications Solutions**
  This document describes the Command Line Interface for Cisco Unified Communications Manager. Some of these commands perform upgrade and installation-related tasks.

For further information about Cisco Unified Communications Manager documentation, refer to the following URL:


The following table lists URLs for software and additional documentation.

<table>
<thead>
<tr>
<th>Related Information and Software</th>
<th>URL</th>
</tr>
</thead>
</table>
### Related Information and Software

<table>
<thead>
<tr>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager service releases</td>
<td><a href="http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml">http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml</a></td>
</tr>
</tbody>
</table>

---

**Note**

The installation procedure is different for MCS 7825 H3 and MCS 7828 H3, when compared to other MCS servers that are mentioned in the Cisco MCS data sheets. For more information, see Step 5 in the topic related to installing the software.

---

**Related Topics**

Install software, on page 22

---

**Conventions**

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td>italic font</td>
<td>Arguments for which you supply values are in italics.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the system displays are in screen font.</td>
</tr>
<tr>
<td><strong>boldface screen</strong> font</td>
<td>Information you must enter is in <strong>boldface screen</strong> font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>
Obtain support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Cisco product security overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.
Cisco Unified CM installation

- Cisco Unified Communications Manager installation, page 3
Installation scenarios

You can use this document to perform the following different installation scenarios:

• Install software from a DVD on the first node
• Install software from a DVD on a subsequent node
Install software from a DVD on the first node

You can install software on the first server or on the first node in a cluster.

Procedure

Step 1  Perform all pre-installation tasks that apply to your site.
Step 2  Follow the procedure to begin installing the software from the DVD to your server.
Step 3  Follow the procedure for performing a basic installation.
Step 4  When the Configuration window displays, choose Yes to configure the new server as the first node.
Step 5  Follow the procedure to configure the first node server.
Step 6  Perform all post-installation tasks that apply to your site.

Related Topics

Install software, on page 22
Basic software installation, on page 29

Install software from a DVD on a subsequent node

You can install software that you have on a DVD to a subsequent node.
Procedure

Step 1 Perform all pre-installation tasks that apply to your site.
Step 2 Follow the procedure to begin installing the software from the DVD to your server.
Step 3 Follow the procedure for performing a basic installation.
Step 4 When the First Node Configuration window displays, choose No to configure the new server as a subsequent node.
Step 5 Follow the procedure to configure a subsequent node in the cluster.
Step 6 Perform all post-installation tasks that apply to your site.

Related Topics

Install software, on page 22
Basic software installation, on page 29
Set up subsequent node, on page 32

Apply a patch during installation of the first node

You can upgrade to a later release by downloading and applying a patch during installation of the first node.

Procedure

Step 1 Perform all pre-installation tasks that apply to your site.
Step 2 Follow the procedure to begin installing the software from the DVD to your server.
Step 3 Follow the procedure to apply a software patch.
Step 4 Follow the procedure for performing a basic installation.
Step 5 When the First Node Configuration window displays, choose Yes to configure the new server as the first node.
Step 6 Follow the procedure to configure the first node in the cluster.
Step 7 Perform all post-installation tasks that apply to your site.

Related Topics

Install software, on page 22
Apply a patch, on page 26
Basic software installation, on page 29

Apply a patch during installation of a subsequent node

You can upgrade to a later release by downloading and applying a patch during installation of a subsequent node.
**Procedure**

**Step 1** Perform all pre-installation tasks that apply to your site.

**Step 2** Follow the procedure to begin installing the software from the DVD to your server.

**Step 3** Follow the procedure to apply a software patch.

**Step 4** Follow the procedure for performing a basic installation.

**Step 5** When the First Node Configuration window displays, choose No to configure the new server as a subsequent node.

**Step 6** Follow the procedure to configure a subsequent node in the cluster.

**Step 7** Perform all post-installation tasks that apply to your site.

**Related Topics**
- Install software, on page 22
- Apply a patch, on page 26
- Basic software installation, on page 29
- Set up subsequent node, on page 32

**Add a new node to an existing cluster**

To add a new node to an existing cluster, perform the following steps.

**Procedure**

**Step 1** Before you make any changes to your existing cluster, be sure that you have a current backup file.

**Step 2** Perform all pre-installation tasks that apply to your site.

**Step 3** Ensure that you have the appropriate number of licenses to support adding a new node.

**Step 4** Before you install the new node, ensure that you have configured the new node on the first node. From Cisco Unified Communications Manager Administration on the first node, choose System > Server and configure the IP address for the subsequent nodes. For more information, see the Cisco Unified Communications Manager Administration Guide.

**Step 5** Record the configuration settings for each server that you plan to install.

**Step 6** Follow the procedure to begin installing the software from the DVD to your server. You must install the same software version on all nodes in the cluster. If you do not have the correct version on DVD, you need to download updated software from Cisco.com.
Step 7  Follow the procedure to perform the basic installation.
Step 8  When the First Node Configuration displays, choose No to configure the new server as a subsequent node.
Step 9  Follow the procedure for configuring a subsequent node.
Step 10 Perform all post-installation tasks that apply to your site.
Step 11 If your cluster is running in mixed mode, ensure that you have your USB key and the latest CTL Client installed on the PC that you use to communicate with the first node. After you finish installing the new node, you will need to update the CTL file on all nodes.

Related Topics
- Install software, on page 22
- Basic software installation, on page 29
- Set up subsequent node, on page 32
- Apply security, on page 35

Reuse the MCS-7828

If you have installed Cisco Unified Communications Manager Business Edition 5000 on an MCS-7828 server, and you decide that you need to migrate to separate Cisco Unified Communications Manager and Cisco Unity Connection environments for increased scalability and capacity, you can reuse that MCS-7828 server to run Cisco Unified Communications Manager in a MCS-7825 cluster. Although you can reuse the server, you must reenter your data on the server manually. You must also obtain another server to run Cisco Unity Connection.

Note
You cannot install Cisco Unified Communications Manager on an MCS-7828 server unless you have previously installed Cisco Unified Communications Manager Business Edition 5000.

To migrate from Cisco Unified Communications Manager Business Edition 5000 to separate Cisco Unified Communications Manager and Cisco Unity Connection environments, perform the following steps.

Procedure

Step 1  Order a single migration SKU (CUCM-BE-MIG). The migration SKU ships with software install media that is required to install Cisco Unified Communications Manager and Cisco Unity Connection. The SKU provides a node license for the Cisco Unified Communications Manager and enables you to migrate the DLU to Cisco Unified Communications Manager.
For ordering information, refer to the Cisco Unified Communications Solutions Ordering Guide.

Step 2  Rehost all device licenses in the Cisco Unified Communications Manager environment by sending a request to licensing@cisco.com. You must include the MAC address (for MCS server deployments) or License MAC (for VMware deployments) and proof of purchase of your devices.

Step 3 Obtain a new server for Cisco Unity Connection.

Step 4 Rehost all voice-messaging and advanced user licenses by sending an email to licensing@cisco.com. You must include the MAC address (for MCS server deployments) or License MAC (for VMware deployments) and proof of purchase of the server on which you plan to install Cisco Unity Connection.

Step 5 Install Cisco Unified Communications Manager on the MCS-7828 server.
Make sure to read this document and the related release notes before beginning the installation.

Step 6  Install Cisco Unity Connection on a new server.
Refer to the Installation Guide for Unity Connection.

Parallel installations of cluster nodes

When you install a cluster, you can begin the installation of the first node and subsequent nodes at the same time. When the installation program prompts you to designate the first node as the first node, stop installing on the subsequent nodes until the installation completes on the first node. Then configure the subsequent node(s) on the first node. You can then continue the installation on the subsequent nodes. For optimal performance, you should choose the Skip option rather than the Proceed option in the installation program.

Pre-installation tasks

Perform all pre-installation tasks to ensure that you can successfully install the Cisco Unified Communications Manager.

Procedure

Step 1  Read this entire document to familiarize yourself with the installation procedure.

Step 2  Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.

Step 3  Ensure that your servers are listed as supported hardware and sized appropriately to support the load of the cluster. Make sure to account for any growth that has occurred since initial system configuration. For information about the capacity of server models, refer to the documentation at http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

Step 4  If you are installing a cluster or adding an node, 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, refer to the Cisco Unified Communications Solution Reference Network Design (SRND) based on Cisco Unified Communications Manager, which you can find at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.

Step 5  If you are getting the system time from an NTP server (mandatory for VMware deployments), verify that the first node can synchronize with the NTP server before you install a subsequent node. Log into the Command Line Interface on the first node and enter the following command: utils ntp status

Note  To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node must be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.

For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Caution  If the first node fails to synchronize with an NTP server, installation of a subsequent node can also fail.

Step 6  If your firewall is not in the routing path, disable the firewall between nodes, if possible. Also, increase the firewall timeout settings until after you complete the installation.
To temporarily allow network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to IP any/any) does not always suffice. The firewall might still close necessary network sessions between nodes due to timeouts.

**Step 7** Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between Cisco Unified Communications Manager nodes.

**Step 8** Record the network interface card (NIC) speed and duplex settings of the switch port to which you will connect the new server.
You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.
Enable PortFast on all switch ports that are connected to Cisco servers. With PortFast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay [the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].

**Step 9** If you use DNS, verify that all servers on which you plan to install Cisco Unified Communications Manager are properly registered in DNS.

**Step 10** Obtain a license file.  
**Note** For more information on specifying the required number of licenses, refer to the *Cisco Unified Communications Manager Administration Guide*.

**Step 11** Record the configurations settings for each server that you plan to install.

**Step 12** For Cisco Unified Communications Manager, configure any subsequent nodes on the first node before you install a subsequent node.
From Cisco Unified Communications Manager Administration on the first node, choose **System > Server** and configure the IP address for the subsequent nodes. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

**Related Topics**
- Verify DNS registration, on page 14
- Licensing, on page 20

**Important considerations**

Before you proceed with the installation, consider the following requirements and recommendations:

- Be aware that when you install on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.

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

  When you install Cisco Unified Communications Manager in a large subnet with a large number of devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.

- Ensure that you connect each Cisco Unified Communications Manager node to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation.
You must connect MCS-7816 and MCS-7825 servers to a UPS in order to prevent file system corruption during power outages.

If you want the Cisco Unified Communications Manager node to automatically monitor UPS signaling and automatically initiate a graceful shutdown upon power loss, you should use specific UPS and server models. For more information on supported models and configurations, refer to the Release Notes for Cisco Unified Communications Manager.

• Install the Cisco Unified Communications Manager software on the first node first and then on the subsequent nodes.

• Make sure that the subsequent node servers that you are installing can connect to the first node server during the installation.

• When you enter the Security password on the first node, be sure that you write it down and save it. You must enter the same password on each subsequent node that you install in the cluster. Install the software during off-peak hours or a maintenance window to avoid impact from interruptions.

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

• Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.

• Do not attempt to perform any configuration tasks during the installation.

• Do not install any Cisco-verified applications until you complete the installation.

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

• Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.

• Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 hours.

• For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings changes made by phone users might get unset. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

• You may encounter a problem during RAID creation when you install Cisco Unified Communications Manager 8.6 or an earlier version on 7825 H3 and 7528 H3 servers that currently have Cisco Unified Communications Manager 9.0 installed on it. To resolve the issue:
  1. Boot the Cisco Unified CM server with the Cisco Unified CM 9.0 recovery disc.
  2. When prompted, choose option C to wipe off all data from the system. Option C indicates “Cleaning the system to set to bare metal state.”
     You can now proceed with the installation of the earlier versions of Cisco Unified CM.

• When you insert or remove a USB drive, you might see error messages on the console similar to “sdb: assuming drive cache: write through.” You can safely ignore these messages.

• Carefully read the information that follows before you proceed with the installation.
Frequently asked questions

The following section contains information about commonly asked questions and responses. Review this section carefully before you begin the installation.

Installation time

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

User name and password requirements

Note

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

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

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

Administrator account user name and password

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

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

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

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

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

Application user name and password

You use the Application User name and password to access applications that are installed on the system, including the following areas:

• Cisco Unified Communications Manager Administration
• Cisco Unified Serviceability
• Real Time Monitoring Tool
• Cisco Unified Reporting

To specify the Application Username and password, follow these guidelines:

• Application Username - The Application 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.

You can change the Application Username 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**

Cisco Unified Communications Manager systems use this password to authorize communications between 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.

**Related Topics**

Password considerations, on page 12

**Password considerations**

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

• Mix uppercase and lowercase letters.
• Mix letters and numbers.
• Include hyphens and underscores.
• Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

• Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
• Do not invert recognizable words.
• Do not use word or number patterns, like aaabbb, qwerty, zyxvwuts, 123321, and so on.
• Do not use recognizable words from other languages.
• Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.
Server support

For information about Cisco Unified Communications Manager supported server models, refer to the following documentation:

- Release notes for your product release

Software restrictions

You must do all software installations and upgrades by using Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Communications Manager with Cisco Unified Communications Manager 9.0(1).

Browser requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified Communications Operating System Administration, and Disaster Recovery System by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 2: Supported Browsers and Operating Systems

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

If you use DNS, verify that all servers to be added are registered in DNS properly by performing the following actions:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open a command prompt.</td>
</tr>
<tr>
<td>Step 2</td>
<td>To ping each server by its DNS name, enter ping DNS_name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To look up each server by IP address, enter nslookup IP_address.</td>
</tr>
</tbody>
</table>

Installation information

Use the following table to record the information about your server. Gather this information for each Cisco Unified Communications Manager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You should 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.

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

Caution
You cannot change some of the fields after 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 field after installation, and if you can, it provides the appropriate Command Line Interface (CLI) command.

Caution
If Cisco Unified Communications Manager is running on VMware, changing some of these values after installation will require you to obtain updated licenses.
### Table 3: Node configuration data

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Can Entry Be Changed After Installation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator ID</td>
<td>This field specifies the administrator account user ID that you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System.</td>
<td>No, you cannot change the entry after installation. <strong>Note</strong> After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>This field specifies the password for the Administrator account, which you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System. Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <strong>CLI &gt; set password admin</strong></td>
</tr>
<tr>
<td>Application User Name</td>
<td>You use the Application User name as the default user name for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <strong>CLI &gt; utils reset_ui_administrator_name</strong></td>
</tr>
<tr>
<td>Application User Password</td>
<td>You use the Application User password as the default password for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <strong>CLI &gt; utils reset_ui_administrator_password</strong></td>
</tr>
<tr>
<td>Country</td>
<td>From the list, choose the appropriate country for your installation.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <strong>CLI &gt; set web-security</strong></td>
</tr>
<tr>
<td>Your entry:</td>
<td><strong>Note</strong> The value you enter gets used to generate a Certificate Signing Request (CSR).</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Can Entry Be Changed After Installation?</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| DHCP              | If you want to use DHCP to automatically configure the network settings on your server, choose Yes. If you choose Yes, you do not get prompted for DNS or static configuration settings. If you choose No, you must enter a hostname, IP Address, IP Mask, and Gateway. | Yes, you can change the entry after installation by using the following CLI command:  
**CLI > set network dhcp** |
| DNS Enable        | A DNS server resolves a hostname into an IP address or an IP address into a hostname. If you do not have a DNS server, enter No. If you have a DNS server, Cisco recommends that you enter Yes to enable DNS.  
**Note** When DNS is not enabled, you should only enter IP addresses (not host names) for all network devices in your Cisco Unified Communications Manager network. | Yes, you can change the entry after installation by using the following CLI command:  
**CLI > set network dns** |
| DNS Primary       | Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd. Consider this field mandatory if DNS is set to yes (DNS enabled). | Yes, you can change the entry after installation by using the following CLI command:  
**CLI > set network dns** |
| DNS Secondary (optional) | Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.                                                                                                                                                        | Yes, you can change the entry after installation by using the following CLI command:  
**CLI > set network dns** |
| Domain            | This field represents the name of the domain in which this machine is located. Consider this field mandatory if DNS is set to yes.                                                                                                                                         | Yes, you can change the entry after installation by using the following CLI command:  
**CLI > set network domain**  
**CLI > set network** |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Can Entry Be Changed After Installation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Address</td>
<td>Enter the IP address of the network gateway.</td>
<td>Yes, you can change the entry after installation by using the following CLI command:</td>
</tr>
<tr>
<td></td>
<td>If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet. If DHCP is set to No, consider this field mandatory.</td>
<td>CLI &gt; set network gateway</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter a host name that is unique to your server.</td>
<td>Yes, you can change the entry after installation. For information, refer to the document Changing the IP Address and Host Name for Cisco Unified Communications Manager for your product release at the following URL: <a href="http://www.cisco.com/en/US/ucts/sw/ps556/prod_maintenance_guides_list.html.voicprod">http://www.cisco.com/en/US/ucts/sw/ps556/prod_maintenance_guides_list.html.voicprod</a>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of your server. If DHCP is set to No, consider this field mandatory.</td>
<td>Yes, you can change the entry after installation. For information, refer to the document Changing the IP Address and Host Name for Cisco Unified Communications Manager for your product release at the following URL: <a href="http://www.cisco.com/en/US/ucts/sw/ps556/prod_maintenance_guides_list.html.voicprod">http://www.cisco.com/en/US/ucts/sw/ps556/prod_maintenance_guides_list.html.voicprod</a>.</td>
</tr>
<tr>
<td>IP Mask</td>
<td>Enter the IP subnet mask of this machine.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: CLI &gt; set network ip eth0</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Can Entry Be Changed After Installation?</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the location of the server. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <code>CLI &gt; set web-security</code></td>
</tr>
<tr>
<td>MTU Size</td>
<td>The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network. Default: 1500 bytes The MTU setting must be the same on all nodes in a cluster.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <code>CLI &gt; set network mtu</code></td>
</tr>
<tr>
<td>NIC Duplex</td>
<td>Choose the duplex mode for the network interface card (NIC), either Full or Half. <strong>Note</strong> This parameter only displays when you choose not to use Automatic Negotiation.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <code>CLI &gt; set network nic</code></td>
</tr>
<tr>
<td>NIC Speed</td>
<td>Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. <strong>Note</strong> This parameter only displays when you choose not to use Automatic Negotiation.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: <code>CLI &gt; set network nic</code></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Can Entry Be Changed After Installation?</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Enter the hostname or IP address of one or more network time protocol (NTP) servers with which you want to synchronize. NTP is required for VMware deployments. You can enter up to five NTP servers.</td>
<td>Yes, you can change the entry after installation by using the Cisco Unified Communications Operating System: Settings &gt; NTP Servers</td>
</tr>
<tr>
<td>Your entry:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node must be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Enter the name of your organization. You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry.</td>
<td>Yes, you can change the entry after installation by using the following CLI command: CLI &gt; set web-security</td>
</tr>
<tr>
<td>Your entry:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> The value you enter gets used to generate a Certificate Signing Request (CSR).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The security password to communicate with one another. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. -------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Save this password. You will be asked to enter the same security password for each subsequent node in the cluster.</td>
<td></td>
</tr>
<tr>
<td>Security Password</td>
<td>Servers in the cluster use the security password to communicate with one another.</td>
<td></td>
</tr>
<tr>
<td>Your entry:</td>
<td></td>
<td>Yes, you can change the entry after installation by using the following CLI command: CLI &gt; set password security</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> To avoid losing communications between nodes, you must change the Security password on all nodes in a cluster and reboot all of the nodes. For more information, refer to the description of this command in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.</td>
<td></td>
</tr>
</tbody>
</table>
### Parameter | Description | Can Entry Be Changed After Installation?
--- | --- | ---
SMTP Location | Enter the hostname or IP address for the SMTP server that is used for outbound e-mail. The hostname can contain alphanumeric characters, hyphens, or periods, but it must start with an alphanumeric character. **Note** You must fill in this field if you plan to use electronic notification. | Yes, you can change the entry after installation by using the following CLI command: `CLI > set smtp`
Your entry: | |
State | Enter the state where the server is located. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR). | Yes, you can change the entry after installation by using the following CLI command: `CLI > set web-security`
Your entry: | |
Time Zone | This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine. | Yes, you can change the entry after installation by using the following CLI command: `CLI > set timezone`
Your entry: | |
Unit | Enter your unit. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR). | Yes, you can change the entry after installation by using the following CLI command: `CLI > set web-security`
Your entry: | |

## Licensing

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of IP phones. See the *Enterprise License Manager User Guide* for information about generating and installing licenses.

## Answer file generator

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to your Cisco Unified Communications Manager product DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
• Provides syntactical validation of data entries.
• Provides online help and documentation.

The following usage requirements apply:
• The web application supports only fresh installs and does not support upgrades.
• If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.

---

**Note**
Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys will have a W95 FAT32 format.

---

**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 can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
• IGNORE - The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box might display multiple times. If you choose to ignore network errors, the installation may fail.

**Installation overview**

The installation process allows you to perform a basic installation or upgrade to a newer service release during the installation.

For a more detailed description of the different installation types, see the following table.
Table 4: Installation Options

<table>
<thead>
<tr>
<th>Installation Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Install</td>
<td>This option represents the basic Cisco Unified Communications Manager 8.6(1) installation, which installs the software from the installation disc and does not use any imported data.</td>
</tr>
<tr>
<td>Applying a Patch (upgrade during install)</td>
<td>This option allows you to upgrade the software version that is contained on the installation disc with a later release. You can only apply one patch during the installation process.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that you have the software image available on DVD or on a remote server prior to choosing this option.</td>
</tr>
</tbody>
</table>

Install new operating system and application

This section describes how to install the operating system and the Cisco Unified Communications Manager application. You install the operating system and application by running one installation program.

Installation wizard

For instructions on how to navigate within the installation wizard, see the following table.

Table 5: Installation wizard navigation

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

Install software

To start the installation, follow this procedure.
If you are installing a subsequent node or adding a node to an existing cluster, you must configure the host name or IP address of the new node on the first node in the cluster. From Cisco Unified Communications Manager Administration on the first node, choose **System > Server** and enter the IP address or host name of the subsequent node. For more information, see the Cisco Unified Communications Manager Administration Guide.

**Note**

Because the Cisco Unified Communications Manager Business Edition 5000 software was preinstalled on the server, you do not need to reinstall the software unless you want to reimagine the server with a later product release. Go directly to the procedure to enter the configuration information.

---

**Procedure**

**Step 1**  
If you have a USB key with configuration information that the Answer File Generator generated, insert it now.

*Note* If you have a new server with the software preinstalled, you do not need to install from a DVD, unless you want to reimagine the server with a later product release. Go directly to the procedure to enter the configuration information.

**Step 2**  
Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

**Step 3**  
To perform the media check, choose **Yes** or, to skip the media check, choose **No**. The media check checks the integrity of the DVD. If your DVD passed the media check previously, you might choose to skip the media check.

**Step 4**  
If you choose **Yes** to perform the media check, the Media Check Result window displays. Perform these tasks:

a) If the Media Check Result displays **Pass**, choose **OK** to continue the installation.

b) If the media fails the Media Check, either download another copy from Cisco.com or obtain another DVD directly from Cisco.

**Step 5**  
The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot:

- First, the installation process checks for the correct drivers, and you may see the following warning:

  ```
  No hard drives have been found. You probably need to manually choose device drivers for install to succeed. Would you like to select drivers now?
  ```

  To continue the installation, choose **Yes**.

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.

- The installation process next verifies RAID configuration and BIOS settings.

  * **Note** If this step repeats, choose **Yes** again.
• If the installation program must install a BIOS update, a notification appears telling you that the system must reboot. Press any key to continue with the installation.

After the hardware checks complete, the Product Deployment Selection window displays.

**Step 6** In the Product Deployment Selection window, select the product to install; then, choose **OK**. You can choose from the following options:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Communications Manager Business Edition 5000 (includes Cisco Unified Communications Manager and Cisco Unity Connection)
- Cisco Enterprise License Manager

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

**Note** As part of this install, Enterprise License Manager is installed automatically. Following the install, Enterprise License Manager can be used to provide simplified, enterprise-wide management of user-based licensing, including license fulfillment. Enterprise License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise level reporting of usage and entitlement. For more information, see the Enterprise License Manager User Guide.

**Step 7** If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.

**Caution** If you choose **Yes** on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

The Platform Installation Wizard window displays.

**Step 8** Choose one of the following options:

- To enter your configuration information manually and have the installation program install the configured software on the server, choose **Proceed** and continue with this procedure.

- To do any of the following tasks, choose **Skip** and perform the procedure to enter the configuration information.

- Manually configure the software that is preinstalled on your server - In this case you do not need to install the software, but you must configure the preinstalled software.

- Perform an unattended installation - In this case, you provide preexisting configuration information on a USB key or floppy disk.

- Install the software before manually configuring it - In this case the installation program installs the software, then prompts you to configure it manually. You can choose **Skip** if you want to reinstall the application on all your servers first and then enter the configuration information at a later time. This method might cause you to spend more time performing the installation than the other methods.

**Step 9** Choose the type of installation to perform by doing the following steps. See Installation overview, on page 21 for more information on installation options.

In the Apply Additional Release window, choose one of the options:
• To upgrade to a later Service Release of the software during installation, choose Yes. Continue to perform the procedure to apply a patch.

• To skip this step, choose No.

• To return to the previous window, choose Back.

Step 10 In the Basic Install window, choose Continue to install the software version on the DVD or configure the preinstalled software. Continue to perform the basic software installation procedure.

---

Related Topics

- Apply a patch, on page 26
- Basic software installation, on page 29
- Enter preexisting configuration information, on page 25

---

Enter preexisting configuration information

Start here if you have a server that has the product preinstalled or if you chose Skip in the Platform Installation Wizard window.

Procedure

Step 1 After the system restarts, the Preexisting Installation Configuration window displays.

Step 2 If you have preexisting configuration information that the Answer File Generator created, that is stored on a floppy disc or a USB key, insert the disc or the USB key now and choose Continue. The installation wizard will read the configuration information during the installation process.

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

The Platform Installation Wizard window displays.

Step 3 To continue with the Platform Installation Wizard, choose Proceed.

Step 4 Choose the type of installation to perform by doing the following steps. See Installation overview, on page 21 for more information on installation options.

In the Apply Additional Release window, choose one of the options:

• To upgrade to a later Service Release of the software during installation, choose Yes. Continue to perform the procedure to apply a patch.

• To skip this step, choose No.

• To return to the previous window, choose Back.

Step 5 In the Basic Install window, choose Continue. Continue to perform the basic software installation procedure.
Related Topics

Apply a patch, on page 26
Basic software installation, on page 29

Apply a patch

If you choose Yes in the Apply a Patch window, the installation wizard installs the software version on the DVD first and then restarts the system. You must obtain the appropriate upgrade file from Cisco.com before you can upgrade during installation.

Note

You can upgrade to any supported higher release, so long as you have a full patch, not an ES or an SR, in which case you can only upgrade to a later service release within the same maintenance release.


You can access the upgrade file during the installation process from either a local disk (DVD) or from a remote FTP or SFTP server.

Procedure

Step 1 The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 2 Choose the upgrade retrieval mechanism to use to retrieve the upgrade file:

- SFTP - Retrieves the upgrade file from a remote server by using the Secure File Transfer Protocol (SFTP). Skip to the Upgrade from a remote server, on page 27.
- FTP - Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the Upgrade from a remote server, on page 27.
- LOCAL - Retrieves the upgrade file from a local DVD. Continue with the Upgrade from a local disk, on page 26.

Upgrade from a local disk

Before you can upgrade from a local disk, you must download the appropriate patch file from Cisco.com and use it to create an upgrade DVD. You must create an ISO image on the DVD from the upgrade file. Just copying the ISO file to a DVD will not work.

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 that is available on the DVD. To update the system with this patch, choose 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, 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 6  When the Apply Patch window displays, choose No.

Step 7  The Windows Upgrade window displays.

Step 8  Choose No and continue with the Basic software installation, on page 29.

---

Upgrade from a remote server

Before you can upgrade from a remote server, you must download the appropriate patch file from Cisco.com to an FTP or SFTP server that the server can access.

If you are upgrading from release 5.1(3), you must download the appropriate patch file from Cisco.com, create an ISO image DVD from the patch file, then copy the contents of the DVD to a remote FTP or SFTP server that the server can access.

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://www.cisco.com/cgi-bin/ctdp/Search.pl. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx. Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (for Unix systems. Refer to http://sshwindows.sourceforge.net/)
- Cygwin (http://www.cygwin.com/)
- Titan (http://www.titanftp.com/)

---

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

---

If you chose to upgrade through an FTP or SFTP connection to a remote server, you must first configure network settings so that the server can connect to the network.
**Procedure**

**Step 1** The Auto Negotiation Configuration window displays.

**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.

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

- To enable automatic negotiation, choose **Yes**.
  
  The MTU Configuration window displays. Skip the next step then continue.

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

**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.

*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 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 6** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Installation information, on page 14 for field descriptions.

The DNS Client Configuration window displays.

**Step 7** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Installation information, on page 14 for field descriptions.

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

**Step 8** 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 9** 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 10** To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

**Step 11** To continue the installation, 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 12** When the Apply Patch window displays, choose **No**.

**Step 13** The Windows Upgrade window displays.

**Step 14** Choose **No** and continue with the Basic software installation, on page 29.

---

### Basic software installation

**Procedure**

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

The Auto Negotiation Configuration window displays.

**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 displays.

  **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 displays.

**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 displays.
- 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. See Installation information, on page 14 for field descriptions.

The DNS Client Configuration window displays.

Step 7  To enable DNS, choose Yes, enter your DNS client information, and choose OK. See Installation information, on page 14 for field descriptions.

The network restarts by using the new configuration information, and the Administrator Login Configuration window displays.

Step 8  Enter your Administrator login and password from Installation information, on page 14.

Note  The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You will need the Administrator login to log in to Cisco Unified Communications Operating System Administration, the command line interface, and the Disaster Recovery System.

The Certificate Information window displays.

Step 9  Enter your certificate signing request information and choose OK.

The First Node Configuration window displays.

Step 10  You can configure this server as either the first node in a Cisco Unified Communications Manager cluster or as a subsequent node.

- To configure this server as the first Cisco Unified Communications Manager node, choose Yes and continue with the Configure the first node.
- To configure this server as a subsequent node in the cluster, choose No and continue with the Set up subsequent node, on page 32.

Step 11  Continue with the Set up first node, on page 31.
Set up first node

After you finish the basic installation, follow this procedure to configure the server as the first node in the cluster.

Procedure

Step 1  The Network Time Protocol Client Configuration window displays. Cisco recommends that you use an external NTP server to ensure accurate system time on the first node. Ensure the external NTP server is stratum 5 or higher (meaning strataums 1-9). Subsequent nodes in the cluster will get their time from the first node.

Note  When you are installing Cisco Unity Connection on a virtual machine, you must specify an external NTP server.

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

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

  Note  If the Test button displays, 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.

Step 3  Enter the Security password from Installation information, on page 14.

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 Database Access Security Configuration window displays.

Step 4  If you want to configure an SMTP server, choose Yes and enter the SMTP server name.

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. The Application User Configuration window displays.

Step 6  Enter the Application User name and password from Installation information, on page 14 and confirm the password by entering it again.

Step 7  Choose OK. The Platform Configuration Confirmation window displays.

Step 8  To continue with the installation, choose OK; or to modify the platform configuration, choose Back. The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.

Step 9  When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 10  Complete the post-installation tasks that are listed in the Post-installation tasks, on page 33.
Set up subsequent node

To configure a subsequent node in the cluster, follow these steps.

⚠️ Caution
You must configure a subsequent node on the first node by using Cisco Unified Communications Manager Administration before you install the subsequent node. For more information, see the Cisco Unified Communications Manager Administration Guide.

Procedure

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

Note If the first node is not synchronized with an NTP server, installation of the subsequent node will fail.

Step 2 On the First Node Configuration window, read the Warning and make sure you have correctly configured the first node. To continue with the installation of the subsequent node, click OK. The Network Connectivity Test Configuration window displays.

Step 3 During installation of a subsequent node, the system checks to ensure that the subsequent node can connect to the first 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 first 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 To start installing the software, choose OK, or, if you want to change the configuration, choose Back.

Step 7 When the installation process completes, you get prompted to log in by using the Administrator account and password.
What to Do Next
Proceed to complete the post-installation tasks.

Related Topics
Post-installation tasks, on page 33

Post-installation tasks

After installing the Cisco Unified Communications Manager on your server, you must set some configuration parameters and perform other post-installation tasks before you can begin using it. Perform these tasks for the server that you install and complete the tasks before other servers in the cluster are installed.

For post-installation tasks that you must complete after the installation, see the following table.

Table 6: Post-Installation Tasks

<table>
<thead>
<tr>
<th>Post-Installation Tasks</th>
<th>Important Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in as the Cisco Unified Communications Manager Application User and change the Application User passwords.</td>
<td>See the Change default application user passwords, on page 34.</td>
</tr>
<tr>
<td>Install Real Time Monitoring Tool.</td>
<td>You can use Real Time Monitoring Tool to monitor system health, and view and collect logs. For installation instructions and more information about Real Time Monitoring Tool, see the Cisco Unified Real Time Monitoring Tool Administration Guide.</td>
</tr>
<tr>
<td>Configure the netdump utility, if you installed a cluster of servers.</td>
<td>The netdump utility allows you to send data and memory crash dump logs from one server on the network to another. For instructions for configuring the netdump utility, refer to the Troubleshooting Guide.</td>
</tr>
<tr>
<td>Upload your Cisco Unified Communications Manager license files to the first node.</td>
<td>See the Install licenses, on page 35.</td>
</tr>
<tr>
<td>Activate Cisco Unified Communications Manager feature services that you want to run.</td>
<td>Refer to Cisco Unified Serviceability Administration Guide. See the Cisco Unified Serviceability, on page 34.</td>
</tr>
<tr>
<td>Configure the backup settings. Remember to back up your data daily.</td>
<td>Refer to Disaster Recovery System Administration Guide.</td>
</tr>
</tbody>
</table>
## Post-installation tasks

<table>
<thead>
<tr>
<th>Post-Installation Tasks</th>
<th>Important Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The locale English United States installs automatically on the server; however, you can add new locales to the server, if required.</td>
<td>Refer to <em>Cisco Unified Communications Operating System Administration Guide</em>.</td>
</tr>
<tr>
<td>Install COP enabler files for any custom device types that you want to use that do not ship with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>If applicable, configure any network management systems in use at your site.</td>
<td>Refer to the <em>Cisco Unified Serviceability Administration Guide</em>.</td>
</tr>
<tr>
<td>If you want to set up a secure cluster, you can run your Cisco IP Telephony network in mixed mode.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Configure the system.</td>
<td>See the <em>Set up database, on page 35</em>.</td>
</tr>
<tr>
<td>For more information, refer to the <em>Cisco Unified Communications Manager System Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>Install Cisco Unified Communications Manager IM and Presence Service.</td>
<td>See <em>Installation overview, on page 63</em>.</td>
</tr>
</tbody>
</table>

### Change default application user passwords

The installation sets all Application User passwords to the same Application User password that you entered during installation. Cisco recommends that you log in to Cisco Unified Communications Manager Administration and change these passwords. Refer to *Cisco Unified Communications Manager Administration Guide* for the procedure for changing a password.

### Cisco Unified Serviceability

To access Cisco Unified Communications Manager Administration or Cisco Unified Serviceability, you will need to use a web browser from a PC with network access to the Cisco Unified Communications Manager server.

Even though all services are installed on each server in the cluster, you must manually activate the services that you want to run on each server in the cluster through Cisco Unified Serviceability. For service recommendations and more information, refer to *Cisco Unified Serviceability Administration Guide*.

### Services activation

Even though all services are installed on the server, you may need to use Cisco Unified Serviceability to manually activate services that you want to run. For service recommendations and more information, see *Cisco Unified Serviceability Administration Guide*. 
Install licenses

See the Enterprise License Manager User Guide for information about generating and installing licenses for Cisco Unified Communications Manager.

Apply security

Use the following procedure to apply security to a new node in a secure cluster after you have successfully added the node. For more information on adding a new node to a cluster, see the Add a new node to an existing cluster, on page 6.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Activate the Cisco CTL Provider service on the new node.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Use an etoken from the existing CTL file and run the CTL client again to get the certificates from all the servers in the cluster, including the new server, into the CTL file. You must be running the Cisco CTL Provider on all servers in the cluster to generate the certificates and update the CTL file.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Restart the Cisco TFTP service on all TFTP servers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Restart the Cisco CallManager service on all the nodes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Reset all devices to distribute the new CTL file to the devices.</td>
</tr>
</tbody>
</table>

Set up database

After installing Cisco Unified Communications Manager, you use Cisco Unified Communications Manager Administration to begin configuring the database. The Cisco Unified Communications Manager database contains information and parameters that relate to the system as a whole, to connected devices, and to individual users. The following list describes a few tasks that you must perform in Cisco Unified Communications Manager Administration or Cisco Unified Serviceability:

1. In Cisco Unified Serviceability, activate the services that you want to run on each server in the cluster.
2. Configure system-level settings, such as Cisco Unified Communications Manager Groups.
3. Design and configure your dialing plan.
4. Configure media resources for conferences, music on hold, and so on.
5. Configure systemwide features, Cisco Unified IP Phone services, Cisco Unified Communications Manager Extension Mobility, Cisco Unified Communications Manager Attendant Console, and Cisco Unified Communications Manager Assistant.
6. Install and configure the gateways.
7. Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
8 Configure the users.
9 Configure and install the phones; then, associate users with the phones.

For more information about configuring the Cisco Unified Communications Manager database, refer to the Cisco Unified Communications Manager Administration Guide, the Cisco Unified Communications Manager System Guide, or online help in the Cisco Unified Communications Manager application.

Log files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

**Command Syntax**

```
file list install *
```

To view the log file from the command line, enter

```
file view install log_file
```

where `log_file` is the log file name.

You can also view logs by using the Real Time Monitoring Tool. For more information on using and installing the Real Time Monitoring Tool, refer to the Cisco Unified Real Time Monitoring Tool Administration Guide.

You can get more information about installation events by viewing or downloading the System History log. Refer to the following for more information:

- Cisco Unified Real Time Monitoring Tool Administration Guide
- Troubleshooting Guide

COP files, dial plans, and locales

This section contains information about COP files, dial plans, and locales.

COP file installation

The following guidelines apply to installing COP files. If the documentation for a specific COP file contradicts these general guidelines, follow the COP file documentation:

- Install the COP file on every server in a cluster.
- After you install a COP file, you must restart the server.

**Note**

You must restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database. Cisco recommends that you perform this restart during an off-peak period.
Dial plan installation

You can install dial plan files from either a local or a remote source by using the same process for installing software upgrades. See the Upgrade Guide for Cisco Unified Communications Manager for more information about upgrading from a local or remote source.

After you install the dial plan files on the system, log in to Cisco Unified Communications Manager Administration and then navigate to Call Routing > Dial Plan Installer to complete installing the dial plans.

Locale installation

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

User Locales

User locale files provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. User-only locale installers exist on the web.

Network Locales

Network locale files provide country-specific phone tones and gateway tones, if available. Network-only locale installers exist on the web.

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

Note

The Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

Changes do not take effect until you reboot every server in the cluster. Cisco strongly recommends that you do not reboot the servers until you have installed all locales on all servers in the cluster. Minimize call-processing interruptions by rebooting the servers after regular business hours.

Install locales

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. See the Upgrade Guide for Cisco Unified Communications Manager for more information about upgrading from a local or remote source.

Note

To activate the newly installed locales, you must restart the server. You can install more than one locale before you restart the server.

Related Topics

Locale files, on page 38
Locale files

When you are installing Cisco Unified Communications Manager locales, you must install the following files:

- User Locale files - Contain language information for a specific language and country and use the following convention:
  
  cm-locale-language-country-version.cop

- Combined Network Locale file - Contains country-specific files for all countries 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

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>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LOCALE] File not found: <code>&lt;language&gt;_ </code>&lt;country&gt;_&lt;userLocale&gt;.csv`, the user locale has not been added to the database.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] File not found: <code>&lt;country&gt;_networkLocale.csv</code>, the network locale has not been added to the database.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Communications Manager CSV file installer installdb is not present or not executable</td>
<td>This error occurs because a Cisco Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified Communications Manager database. If this application is not found, it either was not installed with Cisco Unified Communications Manager (very unlikely), has been deleted (more likely), or the server does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.</td>
</tr>
</tbody>
</table>
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 Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_&lt;ll&gt;_&lt;CC&gt;.properties.Checksum.</td>
<td>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 Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.</td>
</tr>
<tr>
<td>[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Addition of &lt;RPM-file-name&gt; to the Cisco Unified Communications Manager database has failed!</td>
<td>This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.</td>
</tr>
</tbody>
</table>

**Supported products**

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager, which is available at this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51
IM and Presence Service installation

- New in this release, page 43
- Product description, page 45
- Before you begin, page 49
- Installation, page 63
- Post-installation tasks, page 81
- Reference, page 87
New in this release

This chapter describes what is new in this release of Cisco Unified Communications Manager IM and Presence Service.

- Rebranding to IM and Presence, page 43
- Version alignment, page 43
- Centralized profile configuration and data migration, page 44
- Licensing simplification, page 44
- Deprecated features, page 44

Rebranding to IM and Presence

Cisco Unified Presence is now known as the Cisco Unified Communications Manager IM and Presence Service. All GUIs and customer documentation have been rebranded accordingly.

Version alignment

Release 9.0(1) provides a tighter integration between IM and Presence and Cisco Unified Communications Manager (Unified CM). From Release 9.0(1) onwards, IM and Presence and Unified CM software versions must match. For two software versions to match, they must have the same major and minor release number. Major and minor release numbers are defined as follows:

9.x.y

where 9 = major release number, x = minor release number and y = maintenance release number.

For example, IM and Presence Release 9.0.2.10000-1 is compatible with Unified CM Release 9.0.12.30000-3, but it is not compatible with Unified CM Release 9.1.1.10000-5. Similarly, Unified CM Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-1.

For fresh installations, Unified CM 9.0(1) must be installed before IM and Presence 9.0(1) is installed. For upgrades, Unified CM must be upgraded to Release 9.0(1) before IM and Presence is upgraded. Upgrades must be performed within the same maintenance window.
Centralized profile configuration and data migration

From Release 9.0(1), the user UC service profile information for LDAP, Voicemail, Conferencing, Mailstore, CTI Gateway and Audio that was configured from the Application > CUPC/Cisco Jabber menu in Cisco Unified Presence Administration is now configurable on Cisco Unified Communications Manager (Unified CM) from the User Management > User Settings > UC Service and Service Profile menus. Therefore, when you upgrade from Cisco Unified Presence Release 8.x to IM and Presence Release 9.x, all user profile information is migrated to Unified CM. For more information about user migration, see the Upgrade Guide for Cisco Unified Communications Manager.

Licensing simplification

The IM and Presence Service does not require a server license or software version license. IM and Presence is enabled on a per user basis, regardless of the number of clients you associate with each user. Release 9.0(1) supports a centralized user-based licensing system on Unified CM, whereby IM and presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). For more information about license requirements, see the “IM and Presence license requirements” section of this document.

Related Topics

IM and Presence license requirements, on page 47

Deprecated features

Release 9.0(1) does not support the following features:

• Cisco IP Phone Messenger
• Cisco Unified Personal Communicator 7.x
• Cisco Agent Desktop
• Expert Advisor
• Cisco Unified Application Environment
• Cisco Unified Mobile Communicator
• Cisco Unified Mobile Communicator Application
• SIP Proxy Mode
Product description

This chapter describes the IM and Presence Service.

- Overview of IM and Presence, page 45
- Publisher and subscriber nodes, page 45
- Interaction with Cisco Unified Communications Manager, page 46
- IM and Presence license requirements, page 47

Overview of IM and Presence

IM and Presence, which is a service of Cisco Unified Communications Manager, provides native standards-based dual-protocol enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service offers users feature-rich communications capabilities both within and external to the enterprise.

Publisher and subscriber nodes

Before you install IM and Presence, you must install Cisco Unified Communications Manager. From Release 9.0(1), IM and Presence and Cisco Unified Communications Manager software releases must match.

The first node that you install in each IM and Presence cluster is called the publisher node. 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 IM and Presence software on the subscriber nodes.

In multi-node deployments, the order in which you configure the system topology and install new nodes is very important. The order of installation and configuration is as follows:

1. Install and configure the IM and Presence publisher node.
2. On the publisher node, create the IM and Presence subclusters and subscriber nodes in the cluster.
3. Install and configure each of the subscriber nodes in the cluster.
4 On the publisher node, assign the subscriber nodes to the subcluster arrangement as required.

For more information about how to configure the system topology, see the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.

**Related Topics**

Interaction with Cisco Unified Communications Manager, on page 46

---

**Interaction with Cisco Unified Communications Manager**

IM and Presence is a service of Cisco Unified Communications Manager (Unified CM) and is therefore tightly integrated with Unified CM.

From IM and Presence Release 9.0(1) onwards, IM and Presence and Cisco Unified Communications Manager (Unified CM) software versions must match. For two software versions to match, they must have the same major and minor release number. Major and minor release numbers are defined as follows:

9.x.y

where 9 = major release number, x = minor release number and y = maintenance release number.

For example, IM and Presence Release 9.0.2.10000-1 is compatible with Unified CM Release 9.0.12.30000-3, but it is not compatible with Unified CM Release 9.1.1.10000-5. Similarly, Unified CM Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-1.

---

**Note**

You must install Unified CM before you install IM and Presence.

When you install IM and Presence, you must provide the following Unified CM information:

- The Unified CM publisher hostname
- The Unified CM IP address (only for deployments that do not use Domain Name Service (DNS))
- The Unified CM publisher security password
- User ID and password for the Standard AXL API Access role

**Related Topics**

Required installation information, on page 51

---

**System time on IM and Presence publisher node**

When you install the IM and Presence publisher node, you must specify an external Network Time Protocol (NTP) server to ensure that accurate system time is set on the publisher node. Cisco recommends that you configure the Cisco Unified Communications Manager (Unified CM) publisher node as the sole NTP server. This means that all subsequent nodes in the cluster will set the time from the Unified CM server.

If, for some reason, you do not want to set the Unified CM as the NTP server, you must specify at least three other NTP servers and ensure that these servers are stratum 5 or higher. However, regardless of which NTP server(s) you configure during installation of the publisher node, after you complete the post-installation deployment wizard in Cisco Unified CM IM and Presence Administration, the Unified CM will be used to
set the time for all IM and Presence nodes in the cluster to ensure consistent time between Unified CM and IM and Presence.

To verify that the Unified CM publisher’s NTP service is working correctly, you can select **Cisco Unified OS Administration > Settings > NTP Servers** or enter the following CLI command: **utils ntp status**.

**IM and Presence license requirements**

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

**Note**

With the Jabber for Everyone Offer, no end user licenses are required to enable IM and presence functionality. See the *Jabber for Everyone Quick Start Guide, Release 9.0(1)* for more information.

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

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

- The **End User Configuration** window in Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Administration Guide* for more information.

- The Bulk Administration Tool (BAT)

- Assign IM and Presence to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified CM.

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

IM and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence capabilities can also be acquired for users that are not Cisco Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. See the *Jabber for Everyone Quick Start Guide, Release 9.0(1)* for more information.
IM and Presence license requirements
Before you begin

This chapter discusses how you should prepare for the installation of the IM and Presence Service.

- Read this first, page 49
- Installation time requirements, page 50
- System requirements, page 50
- Hardware and software requirements, page 58
- Perform pre-installation tasks, page 58
- Cluster topology, page 59
- Unattended installation of IM and Presence, page 60

Read this first

When you install the IM and Presence Service on an existing server, the hard drive is formatted, and all existing data on the drive is overwritten.

DNS requirements

Note the following DNS requirements:

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

- Unified CM and IM and Presence should use the same DNS server—If you use different DNS servers between IM and Presence and Unified CM, it is likely to cause abnormal system behavior.

- Multi-node considerations—if you are using the multi-node feature in IM and Presence, see the section regarding multi-node deployments in the Deployment Guide for IM and Presence for DNS configuration options.
Installation time requirements

The entire IM and Presence installation process, excluding pre- and post-installation tasks, takes approximately 45 to 120 minutes per server, depending on your server type.

System requirements

Required passwords

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

- Administrator account username and password
- Application username and password
- Security password

Related Topics

Administrator account username and password, on page 50
Application username and password, on page 50
Security password, on page 51

Administrator account username and password

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

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

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

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

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

Related Topics

Required installation information, on page 51

Application username and password

During installation, you must create an Application User user ID and password to sign into the Cisco Unified CM IM and Presence Administration interface.

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

Required installation information, on page 51

Security password

During installation, you must specify a system security password. This password is used to secure communication between cluster nodes. In the Post-Installation deployment wizard, which displays the first time you sign in to Cisco Unified CM IM and Presence Administration, you must reset the security password to be identical to the password used on the Cisco Unified Communications Manager (Unified CM) publisher server.

Note

The security password that you set for IM and Presence in the Post-Installation deployment wizard must be identical to the password used on the Unified CM Publisher server. The system uses this password to authorize communications between nodes, and you must ensure that this password is identical on all nodes in the cluster.

If you lose the Unified CM security password, there is no way to verify from IM and Presence what the security password is on the Unified CM server. See Cisco Unified Communications Manager documentation for information about how to retrieve the security password.

To reset the Unified CM security password after your first sign in to Cisco Unified CM IM and Presence Administration, (for example, if the password has changed on Unified CM and you need to update it on IM and Presence) select **System > CUCM Publisher** from Cisco Unified CM IM and Presence Administration.

Required installation information

When you install the IM and Presence Service on a server, the installation process requires certain information that you must provide. You can provide this information manually during the installation process or you can provide it using an answer file. For each IM and Presence 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 install IM and Presence.

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.

The last column in the table shows whether you can change a parameter after installation, and if you can, if provides the appropriate menu path or Command Line Interface (CLI) command.

<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Credentials</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Required installation information
### Configuration data

<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Login</td>
<td>Specifies the name that you want to assign to the Administrator account.</td>
<td>No</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specifies the password for the Administrator account.</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI: set password admin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Application User Credentials

<table>
<thead>
<tr>
<th>Application User Username</th>
<th>Specifies the user ID for Cisco Unified CM IM and Presence Administration.</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI: utils reset ui administrator name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application User Password</td>
<td>Specifies the password for Cisco Unified CM IM and Presence Administration.</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI: utils reset ui administrator password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Security Password

<table>
<thead>
<tr>
<th>Security password for Cisco Unified Communications Manager publisher node</th>
<th>The security password that you set for each IM and Presence server must be identical to the password used on the Cisco Unified Communications Manager Publisher server.</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can change the security password entered during an initial installation in one of two ways:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• As you configure the post-installation wizard in Cisco Unified CM IM and Presence Administration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• In Cisco Unified CM IM and Presence Administration, select <strong>System &gt; CUCM Publisher</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Certificate Information

<table>
<thead>
<tr>
<th>Organization</th>
<th>Used to create the Certificate Signing Request.</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI: set web-security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI: set web-security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI: set web-security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration data</td>
<td>Description</td>
<td>Editable after installation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set web-security</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set web-security [orgunit] [orgname] [locality] [state]</td>
<td></td>
</tr>
<tr>
<td>(Optional) SMTP</td>
<td>Specifies the name of the SMTP host that is used for outbound email.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.</td>
<td></td>
</tr>
<tr>
<td>SMTP Location</td>
<td>• In Cisco Unified Communications Operating System Administration: select Settings &gt; SMTP and enter the IP address or Hostname in the SMTP Host Field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CLI: set smtp</td>
<td></td>
</tr>
<tr>
<td>NIC Interface Settings</td>
<td>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).</td>
<td>Yes</td>
</tr>
<tr>
<td>NIC Speed</td>
<td>CLI: set network nic</td>
<td></td>
</tr>
<tr>
<td>NIC Duplex</td>
<td>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).</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set network nic</td>
<td></td>
</tr>
<tr>
<td>MTU Size</td>
<td>The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. The MTU setting must be the same on all nodes in a cluster.</td>
<td>Yes</td>
</tr>
<tr>
<td>Note</td>
<td>If you need to change this value for IM and Presence, you must match it with the value on Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>Configuration data</td>
<td>Description</td>
<td>Editable after installation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>Network Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP (Dynamic Host Configuration Protocol)</td>
<td>Select Yes if you want to use DHCP to automatically configure the network settings on your server. If you select No, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration.</td>
<td>Yes.</td>
</tr>
</tbody>
</table>
| | | • In Cisco Unified OS Administration: select Settings > IP > Publisher  
• CLI: set network dhcp |
| Host Name | If DHCP is set to No, you must enter a hostname for this machine. | Yes |
| | | • In Cisco Unified Communications Operating System Administration, select Settings > IP > Ethernet  
• CLI: set network IP |
| IP Address | If DHCP is set to No, you must enter the IP address of this machine. | Yes |
| | | • In Cisco Unified Communications Operating System Administration, select Settings > IP > Ethernet  
• CLI: set network IP eth0 [ip-address] [ip-mask] |
| IP Mask | If DHCP is set to No, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. | Yes |
| | | • In Cisco Unified Communications Operating System Administration, select Settings > IP > Ethernet  
• CLI: set network IP eth0 [ip-address] [ip-mask] |
### Configuration data

<table>
<thead>
<tr>
<th><strong>Configuration data</strong></th>
<th><strong>Description</strong></th>
<th><strong>Editable after installation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Address</td>
<td>If DHCP is set to No, you must enter the gateway address.</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In Cisco Unified Communications Operating System Administration, select <strong>Settings &gt; IP &gt; Ethernet</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CLI: set network gateway</td>
</tr>
<tr>
<td><em>(Optional) DNS</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Primary</td>
<td>If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLI: set network dns primary</td>
</tr>
<tr>
<td>DNS Secondary</td>
<td>When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLI: set network dns secondary</td>
</tr>
<tr>
<td>Domain</td>
<td>Represents the name of the domain in which this machine is located</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLI: set network domain</td>
</tr>
<tr>
<td>Timezone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLI: set timezone</td>
</tr>
</tbody>
</table>

**Network Time Protocol**
<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Server IP Address</td>
<td>During installation of the IM and Presence publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. Cisco recommends that you use the Cisco Unified Communications Manager publisher node as the NTP server.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>In Cisco Unified Communications Operating System Administration, select Settings &gt; NTP Servers</td>
<td></td>
</tr>
<tr>
<td>IM and Presence Publisher Node</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM and Presence Publisher</td>
<td>You need the hostname of the IM and Presence publisher node when you add a subscriber node to a cluster.</td>
<td>Yes</td>
</tr>
<tr>
<td>Note</td>
<td>In Cisco Unified Communications Operating System Administration, select Settings &gt; IP &gt; Publisher</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>This only applies if, for network configuration purposes, you changed the hostname on the IM and Presence publisher server. If you do this, you must update the IP address of the publisher server on subsequent servers in IM and Presence.</td>
<td></td>
</tr>
<tr>
<td>IM and Presence Publisher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node IP Address</td>
<td>If your network does not have DNS, you must provide the IP address of the IM and Presence publisher node when you add a subscriber node to a cluster.</td>
<td>Yes</td>
</tr>
<tr>
<td>Note</td>
<td>In Cisco Unified Communications Operating System Administration: select Settings &gt; IP &gt; Publisher</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>This only applies if, for network configuration purposes, you changed the hostname on the IM and Presence publisher server. If you do this, you must update the IP address of the publisher server on subsequent servers in IM and Presence.</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager Publisher Node</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration data</td>
<td>Description</td>
<td>Editable after installation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Publisher Node Hostname</td>
<td>You need the hostname of the Cisco Unified Communications Manager publisher node when you complete the post-installation deployment wizard for the IM and Presence publisher node.</td>
<td>Yes&lt;br&gt;In Cisco Unified CM IM and Presence Administration, select <strong>System &gt; CUCM Publisher</strong></td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Publisher Node IP Address.</td>
<td>You need the hostname of the Cisco Unified Communications Manager publisher node when you complete the post-installation deployment wizard for the IM and Presence publisher node.</td>
<td>Yes&lt;br&gt;In Cisco Unified CM IM and Presence Administration, select <strong>System &gt; CUCM Publisher</strong></td>
</tr>
</tbody>
</table>

**Cisco Unified Communications Manager AXL Credentials**

| AXL User | AXL is the API that IM and Presence uses to communicate with Cisco Unified Communications Manager. During the installation of the publisher node, you must supply the Cisco Unified Communications Manager AXL username in the post-installation deployment wizard. | Yes<br>In Cisco Unified CM IM and Presence Administration, select **System > CUCM Publisher** |
| AXL Password | During the installation of the publisher node, you must supply the Cisco Unified Communications Manager AXL password in the post-installation deployment wizard. | Yes<br>In Cisco Unified CM IM and Presence Administration, select **System > CUCM Publisher** |
Hardware and software requirements

Hardware requirements

You can find information regarding supported hardware for the following servers:

- IM and Presence server
  For IM and Presence hardware support, see the Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1).

- Cisco Unified Communications Manager server
  For Cisco Unified Communications Manager hardware support, see the Cisco Unified Communications Manager compatibility matrix.

If you are configuring the IM and Presence multi-node feature in your network, review the multi-node hardware recommendations in the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1).

Note
You must ensure that all MCS platforms contain a minimum of 4 GB of RAM.

Software restrictions

IM and Presence can only upload and process software that Cisco Systems approves. You cannot install or use third-party Linux or Windows-based software applications with IM and Presence. You perform valid software installations and upgrades in Cisco Unified Communications Operating System Administration.

For information about software compatibility, see the Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1).

Perform pre-installation tasks

You must complete the following pre-installation tasks before you begin to install the IM and Presence software.

Procedure

Step 1 Ensure that the Cisco Unified Communications Manager (Unified CM) and IM and Presence software versions match.

Step 2 Gather all the information you need to complete the installation and configuration of the IM and Presence software.

Step 3 If you are installing a subscriber node, ensure that you add the subscriber node to the IM and Presence publisher node Cluster Topology.

Step 4 Ensure that the IM and Presence server has network access to the Unified CM publisher server. You can ping Unified CM from other servers.

Step 5 Ensure that you turn on the Cisco AXL Web Service on the associated Unified CM server.
Select **Tools > Service Activation** in Cisco Unified Serviceability.

**Step 6**

If you use DNS, ensure that you have configured the host name of the new IM and Presence server on the DNS server and that the DNS server can resolve the host name of the Unified CM publisher server and of other IM and Presence servers (if any).

**Caution**

Cisco recommends that you use the same DNS servers between IM and Presence and Unified CM. If you use different DNS servers, it is likely to cause abnormal system behavior. Both Unified CM and IM and Presence must either use or not use DNS because Cisco does not support mixed-mode deployments. If you are using the multi-node feature in IM and Presence, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for DNS configuration options.

---

**Related Topics**

- Required installation information, on page 51
- Cluster topology, on page 59
- Interaction with Cisco Unified Communications Manager, on page 46

---

**Cluster topology**

The system automatically assigns the first IM and Presence node that you install as the publisher node. For a multi-node IM and Presence deployment, after you install the publisher node you must create the required subclusters and subscriber nodes in your IM and Presence cluster. You perform the system topology configuration on the IM and Presence publisher node; select **System > Cluster Topology** in Cisco Unified CM IM and Presence Administration.

You must create the subscriber nodes in your topology (on the publisher node) before you install the IM and Presence software on these nodes. However, you cannot assign these subscriber nodes to a subcluster until after you install IM and Presence software on these subscriber nodes. If you assign a subscriber node to a subcluster before you install it, users in remote clusters will not receive availability information. An availability outage will occur until the node is installed.

**Related Topics**

- Perform fresh multi-node installation, on page 78

---

**Deploy multiple nodes in cluster**

A typical process for deploying multiple nodes in a cluster is as follows:

For more information about configuring the cluster topology, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
Procedure

**Step 1** Install the publisher node.
**Step 2** In Cluster Topology, on the publisher node, create all the subclusters and subscriber nodes.
**Step 3** Install each of the subscriber nodes in the cluster.
**Step 4** In Cluster Topology, on the publisher node, assign the subscriber nodes to the subcluster arrangement as required.

Unattended installation of IM and Presence

IM and Presence can be installed unattended using an XML answer file that reads predefined configuration values during the installation process.

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of IM and Presence. You must generate the answer file, copy it to a USB key and use it with the IM and Presence DVD during the installation process.

The generated XML answer file may be quite large, for example, 1 Gigabyte. Therefore, you may need to reformat the USB key to support a large storage capacity before you save the XML file to the USB key.

**Note**

You can only use answer files for fresh installations of IM and Presence and not for upgrades.

To generate an answer file for unattended installation and configuration of IM and Presence you must access the Cisco Unified Communications Answer File Generator at the following URL:


The web application supports the following features:

- Generates and saves answer files for unattended installations on the publisher server and all subsequent servers.
- Provides syntactical validation of data entries.
- Supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.
- Provides online help and documentation.

**Related Topics**

Reformat USB key to FAT32 file system, on page 61

Generate answer file

The following procedure describes how to generate an answer file using the Cisco Unified Communications Answer File Generator.

**Before You Begin**

Gather the required installation and configuration information.
Procedure

**Step 1** Access the Cisco Unified Communications Answer File Generator at the following URL: http://www.cisco.com/web/cuc_afg/index.html.

**Step 2** Enter the required information for the node(s) that you wish to install.
You can specify installation and configuration information for the publisher node and up to 5 subscriber nodes in a cluster.

*Note* If DHCP client is used on the publisher server, and subsequent server answer files are also generated, you must specify the publisher server IP address.

**Step 3** Select *Generate Answer Files*.

**Step 4** Follow the instructions to download the answer file(s).
A separate answer file will be generated for each node that you want to install and configure.

---

**Related Topics**

Required installation information, on page 51

---

**Reformat USB key to FAT32 file system**

You may need to reformat the USB key for the answer file to the FAT32 file system using the Windows XP Disk Management Utility. The FAT file system format provides for larger storage capacity (for example, 1 Gigabyte). You may need to be an Administrator or a member of the Administrators group to perform this procedure.

**Procedure**

**Step 1** Insert the USB key into a USB slot on the Windows XP computer.

**Step 2** Select *Start > Control Panel > Administrative Tools* and double-select *Computer Management*.

**Step 3** Expand the Storage tree and select *Disk Management*.

**Step 4** Right-click the *Removable Disk* icon and select *Format*.

**Step 5** Select *Yes* if you are asked whether you are sure that you want to format this partition.

**Step 6** Select the *File System* and select *FAT32* from the list box.

**Step 7** Select *OK* and *OK* again when you are prompted to format the volume.

---

**Related Topics**

Use answer file to install and configure IM and Presence, on page 70
Unattended installation of IM and Presence
Installation

The following chapter describes the installation procedures for the IM and Presence Service.

- Installation overview, page 63
- Navigation of installation wizard, page 69
- Installation and configuration of IM and Presence, page 69
- Perform fresh multi-node installation, page 78

Installation overview

IM and Presence supports the following installation and configuration options for the publisher and subscriber nodes:

- Unattended installation and configuration of IM and Presence using an answer file
- Manual installation and configuration of IM and Presence
- Configuration of a preinstalled IM and Presence server

Installation and configuration taskflows

The following sections provide an overview of the high-level tasks that you must perform for each of the installation scenarios. Each high-level task also includes a link to another section of the document, which you can follow for detailed information about the task.

Related Topics

- Run unattended installation and configuration of publisher node, on page 64
- Run unattended installation and configuration of subscriber node, on page 65
- Manually install and configure publisher node, on page 66
- Manually install and configure subscriber node, on page 67
- Add new node to existing cluster, on page 68
Run unattended installation and configuration of publisher node

Figure 1: Unattended installation and configuration of the publisher node

The following list contains the steps that you must complete to use an answer file to automatically install and configure the software on the publisher node.

**Procedure**

- **Step 1** Perform all pre-installation tasks that apply to your site.
- **Step 2** Follow the procedure to use an answer file for unattended installation on the publisher node.
- **Step 3** Follow the procedure to run the post-installation deployment wizard on the publisher node.
- **Step 4** Perform all post-installation tasks that apply to your site.

**Related Topics**

- Perform pre-installation tasks, on page 58
- Use answer file to install and configure IM and Presence, on page 70
- Run post-installation deployment wizard, on page 74
- Perform post-installation tasks, on page 81
Run unattended installation and configuration of subscriber node

Figure 2: Unattended installation and configuration of a subscriber node

The following list contains the steps that you must complete to use an answer file to automatically install and configure the software on a subscriber node.

Procedure

**Step 1** Perform all pre-installation tasks that apply to your site.

**Step 2** Follow the procedure to use an answer file for unattended installation on a subscriber node.

**Step 3** Perform all post-installation tasks that apply to your site.

Related Topics

- Perform pre-installation tasks, on page 58
- Use answer file to install and configure IM and Presence, on page 70
- Perform post-installation tasks, on page 81
Manually install and configure publisher node

Figure 3: Manual installation and configuration of the publisher node

The following list contains the steps that you must complete to install and manually configure the software that you have on a DVD on the publisher node.

Procedure

Step 1 Perform all pre-installation tasks that apply to your site.
Step 2 Follow the procedure to begin installing the software from the DVD to your server.
Step 3 Follow the procedure to configure a basic installation.
Step 4 Follow the procedure to configure the publisher node in the cluster.
Step 5 Follow the procedure to run the post-installation deployment wizard on the publisher node.
Step 6 Perform all post-installation tasks that apply to your site.

Related Topics

Perform pre-installation tasks, on page 58
Start basic installation, on page 70
Configure basic installation, on page 72
Configure publisher node, on page 73
Run post-installation deployment wizard, on page 74
Perform post-installation tasks, on page 81
Manually install and configure subscriber node

The following list contains the steps that you must complete to install and manually configure the software that you have on a DVD on a subscriber node.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Perform all pre-installation tasks that apply to your site.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Follow the procedure to begin installing the software from the DVD to your server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Follow the procedure to configure a basic installation.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Follow the procedure to configure a subscriber node in the cluster.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Perform all post-installation tasks that apply to your site.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Perform pre-installation tasks, on page 58
- Start basic installation, on page 70
- Configure basic installation, on page 72
- Configure subscriber node, on page 75
- Perform post-installation tasks, on page 81
Add new node to existing cluster

The following list contains the steps that you must complete to add a new node to an existing cluster.

**Procedure**

**Step 1** Before you make any changes to your existing cluster, ensure that you have a current backup file. See *Disaster Recovery System Administration Guide*.

**Step 2** Perform all pre-installation tasks that apply to your site.

**Step 3** Before you install the new node, ensure that you have configured it on the publisher node.

**Step 4** You must install the same software version on all nodes in the cluster. Verify that you have the correct version on DVD.

**Step 5** For an unattended installation and configuration of the new node, follow the procedure to use an answer file for the subscriber node installation and configuration.

**Step 6** To manually install and configure the subscriber node, complete the following procedures:

a) Follow the procedure to begin installing the software from the DVD to your server.
b) Follow the procedure to configure a basic installation.
c) Follow the procedure to configure a subscriber node in the cluster.

**Step 7** Perform all post-installation tasks that apply to your site.

**Related Topics**

- Perform pre-installation tasks, on page 58
- Cluster topology, on page 59
- Use answer file to install and configure IM and Presence, on page 70
Navigation of installation wizard

The following table describes how to navigate within the installation wizard.

**Table 9: Installation wizard navigation**

<table>
<thead>
<tr>
<th>To do this</th>
<th>Select this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next field</td>
<td>Tab or right arrow</td>
</tr>
<tr>
<td>Move to the previous field</td>
<td>Alt-Tab or left arrow</td>
</tr>
<tr>
<td>Select an option</td>
<td>Space bar or Enter</td>
</tr>
<tr>
<td>Scroll up or down a list</td>
<td>Up or down arrow</td>
</tr>
<tr>
<td>Go to the previous window</td>
<td>Space bar or Enter when you select Back (when available)</td>
</tr>
<tr>
<td>Get help information for a window</td>
<td>Space bar or Enter when you select Help (when available)</td>
</tr>
</tbody>
</table>

Installation and configuration of IM and Presence

**Media check**

When the installation wizard begins you are prompted to perform a media check. After the media check completes the result of the check is displayed in the Media Check Result window.

If the media check passes, you can continue with the installation. The system installer then performs various hardware checks to ensure your system is correctly configured for IM and Presence. The system installer also checks whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it to Cisco Support. For a list of the supported hardware for IM and Presence, see *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*.

If the media check fails, you have two options. You can continue with the installation, which may fail, or you can start the installation again after you download another copy from Cisco.com or obtain another disk directly from Cisco Systems.
Use answer file to install and configure IM and Presence

You can use an answer file for a fresh installation of IM and Presence. This option will complete the installation and configuration of IM and Presence unattended.

Before You Begin

• Perform the pre-installation tasks.
• Generate the answer file and save it onto a FAT32 file system USB key.

Procedure

Step 1 Insert the USB key into a USB port.
Step 2 Insert the installation DVD into the tray and restart the server, so it starts from the DVD.
Step 3 Select Yes to perform a media check after the server completes its boot sequence.
Step 4 If the media check result is Pass, select OK to continue the installation. Otherwise, you can restart the installation later with a new software disk.
Step 5 In the Product Deployment Selection window, select OK to install Cisco Unified Presence. The installation process then verifies RAID configuration and BIOS settings. If the installation process makes any changes to your hardware configuration settings, you will be prompted to restart your system.
Step 6 In the Proceed with Install window, select Yes to continue with the installation.
Caution Do not select Yes unless you are certain you want to proceed with the installation. If you select Yes in the Proceed with Install window, all existing data on your hard drive will be overwritten and destroyed. The Proceed with Install window indicates the IM and Presence software version, if any, on your hard drive and the version on the DVD.
The IM and Presence software is installed and configured based on the information provided in the answer file.

What to Do Next

• If this is the publisher node, run the post-installation deployment wizard.
• If this is a subscriber node, perform the post-installation tasks.

Related Topics

Perform pre-installation tasks, on page 58
Unattended installation of IM and Presence, on page 60
Run post-installation deployment wizard, on page 74
Perform post-installation tasks, on page 81

Start basic installation

This procedure is the first step in manually installing and configuring IM and Presence software.
Before You Begin

- Perform the pre-installation tasks.
- If you have a new server with IM and Presence preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. Skip to the procedure that describes how to enter preexisting installation data.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Insert the installation DVD into the tray and restart the server, so it starts from the DVD.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select Yes to perform a media check after the server completes its boot sequence.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>If the media check result is Pass, select OK to continue the installation. Otherwise, you can restart the installation later with a new software disk. <strong>Tip</strong> During the hardware checks, the installation process checks for the correct drivers. If you see the following warning “Drivers not found, do you want to install manually?”, you must select Yes to continue with the installation.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the Product Deployment Selection window, select OK to install IM and Presence. The installation process then verifies RAID configuration and BIOS settings. If the installation process makes any changes to your hardware configuration settings, you will be prompted to restart your system.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the Proceed with Install window, select Yes to continue with the installation, otherwise select No. <strong>Caution</strong> Do not select Yes unless you are certain you want to proceed with the installation. If you select Yes in the Proceed with Install window, all existing data on your hard drive will be overwritten and destroyed. The Proceed with Install window indicates the IM and Presence software version, if any, on your hard drive and the version on the DVD.</td>
</tr>
</tbody>
</table>
| **Step 6** | In the Platform Installation window, select one of the following:  
  - **Proceed**—to install and configure the software now.  
  - **Skip**—to install the software now but configure it later. The system will restart and you can continue with the configuration later. |
| **Step 7** | In the Apply Patch window, select No to install the software on the DVD without upgrading to a later release. The option to upgrade to a later release of the software is currently not supported. |
| **Step 8** | Select Continue in the Basic Install window. |

What to Do Next

- Configure the basic installation.
- Configure the pre-installed Cisco Unified Presence server.

Related Topics

- Perform pre-installation tasks, on page 58
- Configure pre-installed IM and Presence server, on page 77
- Configure basic installation, on page 72
Configure basic installation

Before You Begin

• Load your IM and Presence DVD and start the basic installation.

• IM and Presence configuration is specific to your installation requirements, and some fields are optional. For example, you may choose to configure static IP address values and DNS over DHCP.

Procedure

Step 1 In the Timezone Configuration window, select the appropriate timezone for the server and select OK.

Step 2 In the Auto Negotiation Configuration window, select Yes to automatically set the speed and duplex settings of the Ethernet network interface card (NIC).

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

   Otherwise, select No and manually select the appropriate NIC Speed and Duplex settings. Select OK to continue.

Step 3 If you need to change the default Maximum Transit Unit (MTU) value, select Yes, enter the same MTU value that is set on Cisco Unified Communications Manager and select OK.

   Note   If you do not enter the same MTU value as Cisco Unified Communications Manager, the installation will fail.

Step 4 In the DHCP Configuration window, select:

   • Yes to use Dynamic Host Configuration Protocol (DHCP) and continue with Step 7.

   • No to set up a static IP address for the server.

Step 5 In the Static Network Configuration window, enter your static network configuration values and select OK.

Step 6 In the DNS Client Configuration window, select:

   • Yes if you are using DNS, enter your DNS client information and select OK.

   • No if you are not using DNS.

   Note   If you do not use DNS, you must update the IM and Presence node name to be a resolvable value after installation is complete.

Step 7 Enter your Administrator Login and Password credentials.

Step 8 In the Certificate Information window, enter your certificate signing request information (Organization, Unit, Location, State and Country) and select OK to continue.

What to Do Next

• If this is the publisher node, configure the publisher node.

• If this is a subscriber node, configure the subscriber node.
Configure publisher node

Before You Begin

- Start a basic installation.
- Configure the basic installation.

Procedure

Step 1 In the First Node Configuration window, select Yes.
Step 2 In the Network Time Protocol Client Configuration window, enter the IP address, NTP server name, or NTP server pool name of the Cisco Unified Communications Manager publisher node.
Step 3 Enter the Security password in the Security Password window and select OK.
   Note The Security password must be identical to the Cisco Unified Communications Manager Publisher password. You can change the security password the first time you sign in to Cisco Unified CM IM and Presence Administration.
Step 4 If you want to configure an SMTP host, select Yes, enter the SMTP location and select OK.
   Note You must configure an SMTP server to use certain operating system features. However, you can also configure an SMTP server later using either the Cisco Unified Communications Operating System interface or the CLI.
Step 5 In the Application User Configuration window, enter the Application User Username and Application User Password and select OK.
Step 6 In the Platform Configuration Confirmation window, select OK to continue installing the software. After you select OK, you will no longer be able to modify the Platform configuration. When the installation process completes, you are prompted to sign in to the Cisco Unified CM IM and Presence Administration GUI with the Administrator user ID and password.

What to Do Next

Run the post-installation deployment wizard.

Related Topics

- Start basic installation, on page 70
- Configure basic installation, on page 72
- System time on IM and Presence publisher node, on page 46
- Run post-installation deployment wizard, on page 74
Run post-installation deployment wizard

Caution
Always run the post-installation deployment wizard immediately after a fresh installation of the IM and Presence Service, and before you back up or restore your data in the Disaster Recovery System. The operation fails if you install IM and Presence and attempt to back up or restore data in the Disaster Recovery System before you run the post-installation deployment wizard.

You cannot run the post-installation deployment wizard a second time. After you run the post-installation deployment wizard, the next time you sign in to Cisco Unified CM IM and Presence Administration, the application automatically detects that the post-installation configuration is complete and the Cisco Unified CM IM and Presence Administration window displays by default.

There is only one publisher in an IM and Presence cluster, which is the first server that you install. You are required, only once after a fresh installation of the publisher server, to configure the Cisco Unified Communications Manager Publisher and AXL information on the IM and Presence publisher server.

To allow you to do this, a post-installation deployment wizard starts the first time you sign into IM and Presence Administration after a fresh installation of IM and Presence.

Note
When the post-installation deployment wizard launches, it is confirmation that your initial installation has succeeded.

Before You Begin

- Obtain the user ID and password for the application user on Cisco Unified Communications Manager who has AXL permissions.
- If you are not using DNS, obtain the IP address of Cisco Unified Communications Manager publisher.

Procedure

Step 1
Sign into Cisco Unified CM IM and Presence Administration on the publisher node. The post-installation deployment wizard automatically displays. See Access Cisco Unified CM IM and Presence Administration, on page 88 for more information about how to sign into Cisco Unified CM IM and Presence Administration.

Step 2
In the first page of the post-installation deployment wizard, enter the Cisco Unified Communications Manager publisher hostname in the Hostname field.
If your network does not have DNS, enter the Cisco Unified Communications Manager publisher IP address in the IP address field.

Note
If your network does not have DNS, you must enter an IP address because the hostname will not automatically resolve to an IP address. If the hostname can resolve to an IP address using DNS, you can leave the IP address blank and the application detects the IP address automatically.

Step 3
In the second page of the post-installation deployment wizard, enter the user ID and password for the appropriate application user, who is assigned the Standard AXL API Access role on the associated Cisco Unified Communications Manager publisher server.

Note
By default, the Standard AXL API Access role is assigned to the CCM Administrator User ID.
Step 4  In the third page of the post-installation deployment wizard change and confirm the security password provided during the initial installation of the IM and Presence Service. Select **Next**.

*Note* When installing subsequent IM and Presence servers, those subscriber servers will use this new security password and not the one used during the installation of the IM and Presence publisher server.

Step 5  In the fourth page of the post-installation deployment wizard, view your configuration information and select **Confirm** to proceed. Otherwise, select **Back** to correct an error.

Step 6  In the fifth page of the post-installation deployment wizard, select which window you would like to view next within Cisco Unified CM IM and Presence Administration.

**Troubleshooting Tips**

- If an error message displays, check that AXL is running on Cisco Unified Communications Manager and that you have the correct User ID and password. Using a browser, enter `http://<<CUCM Hostname>>/axl`. You will be prompted for the User ID and password. If the details that you enter are correct, a web page displays confirmation that AXL is running and ready to receive requests.

- You cannot run the post-installation wizard a second time. If you need to change the Cisco Unified Communications Manager publisher address or AXL information after this initial configuration, select **System > CUCM Publisher** in Cisco Unified CM IM and Presence Administration.

- Subscriber nodes on IM and Presence will obtain the Cisco Unified Communications Manager publisher information from the publisher node following the configuration checks on the publisher node.

- IM and Presence displays a warning if you perform an installation on discontinued hardware. IM and Presence supports a bridged upgrade from the discontinued hardware. The bridged upgrade permits you to perform a Disaster Recovery System (DRS) backup on the discontinued hardware, and then restore the DRS backup on supported hardware. For more information about bridged upgrades, see the *Upgrade Guide for IM and Presence*. For more information about DRS backups, see the *Disaster Recovery System Administration Guide*.

**What to Do Next**

Perform the post-installation tasks.

**Related Topics**

- Perform post-installation tasks, on page 81
- Access Cisco Unified CM IM and Presence Administration, on page 88

**Configure subscriber node**

When you install a subsequent IM and Presence server, you must associate the subsequent server with the IM and Presence publisher server and configure its hostname and IP address. Each new server must also have network access to the IM and Presence publisher server.

*Note* If you assign a subsequent IM and Presence server to a subcluster before you install it, users in remote clusters will not receive presence information. A presence outage will occur until the server is installed.
You are prompted, before you install any additional IM and Presence servers, to use the Network Connectivity Diagnostic tool to probe the network for connectivity issues. Anomalies will be reported back to you via logs if the system can not verify network access to the publisher server on IM and Presence. If you need to investigate a server problem before proceeding further, you are given an opportunity to pause the process between configuration steps.

**Before You Begin**

- If you are deploying two or more servers in your IM and Presence installation, you must use the multi-node feature in IM and Presence and ensure that your hardware is compatible with this feature. This is necessary for both a fresh installation or upgrade of IM and Presence.
- Ensure that you have configured the publisher server on IM and Presence and the post-installation deployment wizard has run successfully. As you install subsequent servers, consider the original publisher server that you installed as the First Node.
- Add the subscriber node in the Topology view of the publisher node before you install it. Do not assign the subsequent server to a subcluster until after you install it.

**Note**

To configure a subscriber node on the IM and Presence publisher server, select **Cluster > Topology** in Cisco Unified CM IM and Presence Administration. You can add multiple subscriber nodes in one step in the Topology window. For example, if you are installing a multi-node cluster containing six servers including the publisher node, you can add five subscriber nodes to the IM and Presence system topology simultaneously.

- Start a basic installation.
- Configure the basic installation.

**Procedure**

**Step 1**  
In the **First Node Configuration** window, select No.

**Step 2**  
Read the warnings and select OK to continue.

**Step 3**  
Select No to confirm that you want the installation to proceed after the Network Connectivity Test validating is complete.

**Step 4**  
Select Continue when the network connectivity to the publisher server is verified as successful.

**Step 5**  
Enter the following information in the **First Node Access Configuration** window and then select OK to continue:

- Hostname of the IM and Presence publisher server
- IP address of the IM and Presence publisher server
- Security password of the Cisco Unified Communications Manager publisher node

**Note**  
The security password that you set for IM and Presence must be identical to the password used on the Cisco Unified Communications Manager publisher server.

**Step 6**  
If you want to configure an SMTP host, select Yes in the **SMTP Host Configuration** window and enter the SMTP location.
You must configure an SMTP server to use certain operating system features. However, you can also configure an SMTP server later using either the Cisco Unified Communications Operating System interface or the CLI.

**Step 7** In the **Platform Configuration Confirmation** window, select **OK** to start installing the software. Otherwise, select **Back** to change the configuration. When the installation process completes, you are prompted to sign into IM and Presence Administration with the Administrator account and password.

---

**What to Do Next**

Perform the post-installation tasks.

**Related Topics**

- Start basic installation, on page 70
- Configure basic installation, on page 72
- Perform fresh multi-node installation, on page 78
- Perform post-installation tasks, on page 81

---

**Configure pre-installed IM and Presence server**

**Before You Begin**

Start a basic IM and Presence installation, and continue here if you:

- decided to install the IM and Presence software earlier but selected **Skip** in the **Platform Installation Wizard** window to configure it at this later stage
- have a server that has IM and Presence preinstalled

**Procedure**

**Step 1** Perform this action after the system restarts, and the **Preexisting Installation Configuration** window displays:

- If you have preexisting configuration information, generated by the Answer File Generator, that is stored on a USB key, insert the USB key now and select **Continue**. The Installation wizard will read the configuration information during the installation process.

**Step 2** Select **Proceed** in the Platform Installation Wizard.

**Step 3** In the **Apply Patch** window, select **No** to install the software on the DVD without upgrading to a later release. The option to upgrade to a later release of the software is currently not supported.

**Step 4** Select **Continue** in the **Basic Install** window.

**What to Do Next**

- If you used an answer file and this is the publisher node, run the post-installation deployment wizard.
• If you used an answer file and this is the subscriber node, then installation and configuration of the software is complete and you should now perform the post-installation tasks.

• If you did not use an answer file, configure the basic installation.

Related Topics

Run post-installation deployment wizard, on page 74
Perform post-installation tasks, on page 81
Configure basic installation, on page 72

Perform fresh multi-node installation

We recommend that you follow this sequence of tasks when you are configuring your multi-node IM and Presence deployment. You configure the IM and Presence multi-node feature, and manage your subclusters, nodes and users in Cluster Topology in Cisco Unified CM IM and Presence Administration. Select System > Cluster Topology in Cisco Unified CM IM and Presence Administration to access Cluster Topology.

You can create the subscriber nodes in your topology before you install these subscriber nodes, specifically before you install the IM and Presence software on these nodes. However, you cannot assign these subscriber nodes to a subcluster before you install IM and Presence software on these subscriber nodes.

Before You Begin

• Determine the type of multi-node deployment model that you are going to configure.

• Perform the multi-node configuration for your IM and Presence deployment on the IM and Presence publisher node.

Restriction

Your hardware must comply with the multi-node hardware recommendations.

Procedure

Step 1 Install and configure Cisco Unified Communications Manager.

Step 2 Install and configure the IM and Presence publisher node (the first server in the IM and Presence cluster).

Step 3 (On the publisher node) In Cluster Topology, create all subclusters and nodes in the cluster.

Step 4 (On the publisher node) In Cluster Topology, associate each of the subscriber nodes in the cluster with the publisher node.

Step 5 Install and configure each of the subscriber nodes in the cluster.

Step 6 (On the publisher node) In Cluster Topology, assign these nodes to the subcluster arrangement as required.

Note Before you assign or move a node to a subcluster, check the following

• From the System troubleshooter page, verify that the Cisco Replication Watcher service is running on all nodes.

• On the Network services screen in Cisco Unified Serviceability (on the subscriber node), verify that all IM and Presence services are running.
Step 7  Turn on high-availability in the subclusters as required. See the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager for more information.

Step 8  Turn on the Sync Agent service on the publisher node to synchronize with the Cisco Unified Communications Manager user and device configuration information.

Step 9  When the synchronization is complete, turn on the Cisco Presence Engine and the Cisco SIP Proxy services, and verify that the Cisco XCP Router service is turned on.

Step 10 Turn on the XCP services applicable to the features in your deployment. See the documentation for those features to determine what XCP services you must turn on.

Troubleshooting Tips

• The Cisco XCP Router must be running for all availability services to function properly on IM and Presence (both SIP-based and XMPP-based client messaging).

• Before you perform the installation of a subscriber IM and Presence node, you must associate the subscriber node in the Cluster Topology view of the publisher node.

• Do not assign the subscriber node to a subcluster until after you install it. If you assign a subscriber IM and Presence node to a subcluster before you install it, users in remote clusters will not receive availability information. An availability outage will occur until you install the subscriber node.

• If you assign a node before you start the IM and Presence services, there is a possibility that users will not be able to sign in to Cisco Jabber. If this scenario occurs, restart the Cisco Client Profile Agent service. To start or restart IM and Presence services, select Cisco Unified Serviceability > Tools > Control Center - Network Services.

• You must turn off high-availability in a subcluster before you move or unassign a node in that subcluster.

• The Cisco Replication Watcher service delays feature service startup on subscriber nodes if IDS replication is not successfully established.

What to Do Next

(On the publisher node) Configure any intercluster peer relationships with remote IM and Presence clusters. See the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager for more information.
Perform fresh multi-node installation
CHAPTER 6

Post-installation tasks

The following chapter describes the post-installation tasks for the IM and Presence Service.

- Perform post-installation tasks, page 81

Perform post-installation tasks

Figure 6: Post-installation flowchart

Complete the following tasks, in sequence, on each server that you install in an IM and Presence cluster.

Before You Begin

Run the post-installation deployment wizard and set the Cisco Unified Communications Manager Publisher address and AXL parameters on the IM and Presence publisher server.
Procedure

Step 1  Check for software and firmware updates for IM and Presence on Cisco.com.
Step 2  Configure Cisco Unified Communications Manager as a Presence Gateway.
Step 3  Configure a SIP Publish trunk on Cisco Unified Communications Manager.
Step 4  Assign users to servers.
Step 5  Activate Services.
Step 6  For non-DNS deployments, change the IM and Presence node name.
Step 7  For non-DNS deployments, change the default proxy domain name.

Caution  Ensure that you complete this post-installation checklist on the IM and Presence publisher server before you install subsequent IM and Presence servers.

Related Topics

- Run post-installation deployment wizard, on page 74
- Software and firmware updates, on page 82
- Configure Cisco Unified Communications Manager as Presence Gateway, on page 83
- Configure SIP Trunk on Cisco Unified Communications Manager, on page 84
- User and server assignments, on page 84
- Activate services, on page 84
- Change of IM and Presence node name to resolvable value, on page 85
- Change of default Presence domain name, on page 85

Software and firmware updates

After you install IM and Presence, check to see if Cisco has released software upgrades, firmware upgrades, critical patches or Service Updates.

Apply latest Firmware upgrade

To prevent catastrophic failures, apply the latest comprehensive Firmware Upgrade CD (FWUCD) as soon as possible.
### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Browse to <a href="http://www.cisco.com">www.cisco.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Support &gt; Download Software.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Navigate to Products &gt; Voice and Unified Communications &gt; Communications Infrastructure &gt; Voice Servers &gt; Cisco 7800 Series Media Convergence Servers (or Cisco UCS B-Series Blade Servers) &gt; (your server model).</td>
</tr>
<tr>
<td>Step 4</td>
<td>If there is a Firmware Upgrade, follow the instructions to download and apply the latest Firmware Upgrade.</td>
</tr>
</tbody>
</table>

### Check for software upgrades

Service Updates (SUs), contain fixes that were unavailable at the time of the original release. They often include security fixes, firmware updates, or software fixes that could improve operation.

Complete the following procedure to check for software upgrades, Service Updates, critical patches, from www.cisco.com.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Browse to <a href="http://www.cisco.com">www.cisco.com</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Support &gt; Download Software.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Navigate to Products &gt; Voice and Unified Communications &gt; Unified Communications Applications &gt; Cisco Unified Presence &gt; Cisco Unified Presence Version &lt;the version for your deployment&gt;.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If there are any software upgrades, follow the instructions to download the software.</td>
</tr>
</tbody>
</table>

### What to Do Next

Configure the Cisco Unified Communications Manager as a Presence gateway.

### Related Topics

Configure Cisco Unified Communications Manager as Presence Gateway, on page 83

## Configure Cisco Unified Communications Manager as Presence Gateway

### Note

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

- You must configure Cisco Unified Communications Manager as a Presence Gateway on IM and Presence to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and IM and Presence.
- For more information about how to configure a Presence Gateway on IM and Presence, see the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.
What to Do Next
Configure a SIP Trunk on a Cisco Unified Communications Manager.

Related Topics
Configure SIP Trunk on Cisco Unified Communications Manager, on page 84

Configure SIP Trunk on Cisco Unified Communications Manager

• After you configure Cisco Unified Communications Manager as a Presence Gateway, you must configure a SIP PUBLISH trunk on Cisco Unified Communications Manager. See the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager for more information.

• When you have configured the SIP PUBLISH trunk on Cisco Unified Communications Manager, you must then enable SIP PUBLISH on IM and Presence. See the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager for more information.

Related Topics
User and server assignments, on page 84

User and server assignments

User assignment is automatically enabled as a service parameter in Cisco Unified CM IM and Presence Administration. For more information about automatic and manual assignment of users in Cluster Topology, see the Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.

Related Topics
Activate services, on page 84

Activate services

You must activate the following services:

• Cisco SIP Proxy
• Cisco Presence Engine
• Cisco Sync Agent
• Cisco XCP Connection Manager
• Cisco XCP Authentication Service

You must wait until the Cisco Sync Agent is active before you can use the IM and Presence server. 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.
Change of IM and Presence node name to resolvable value

This topic only applies to those deployments that do not use DNS.

During installation, if you select not to use DHCP, you must enter a hostname and IP address for the IM and Presence server. The hostname cannot be null, localhost, or an IP address. The IM and Presence node name gets its value from the hostname that you enter during installation and it must be resolvable. If you do not use DNS in your deployment, then the IM and Presence node name is not resolvable. To overcome this, you must change the IM and Presence node name to be a resolvable value after installation is complete.

For information about how to change the IM and Presence node name, see Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.

Change of default Presence domain name

This topic only applies to those deployments that do not use DNS.

If your IM and Presence deployment does not use DNS, the Presence domain name is set to DOMAIN.NOT.SET during installation. Cisco recommends that you change this value to the enterprise domain value after installation is complete.

Before you change the domain name, you must stop the following services on all nodes in the cluster:

- Cisco Presence Engine—select Cisco Unified Serviceability > Tools > Control Center - Feature Services.
- Cisco Proxy—select Cisco Unified Serviceability > Tools > Control Center - Feature Services.
- Cisco XCP Router—select Cisco Unified Serviceability > Tools > Control Center - Network Services.

For information about how to change the default presence domain name, see IP Address, Domain and Hostname for IM and Presence Service on Cisco Unified Communications Manager.

After you change the default domain name, you can restart the Cisco Presence Engine, Cisco Proxy and Cisco XCP Router services.
Perform post-installation tasks
Reference

This chapter contains reference information about the IM and Presence Service.

- RAID and BIOS settings, page 87
- Access Cisco Unified CM IM and Presence Administration, page 88

RAID and BIOS settings

During the software installation, the system installer configures the system BIOS and RAID settings for the new operating system and IM and Presence Service.

See the following tables for the BIOS settings and the RAID settings that are set up during installation. If the hardware configuration process fails during installation, you can use boot-time utilities on both the IBM and HP servers to manually configure the RAID and BIOS settings, as advised in the following tables.

Table 10: BIOS Configuration Settings for HP and IBM Servers

<table>
<thead>
<tr>
<th>HP Servers</th>
<th>IBM Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Selection: Linux (not applicable on newer models)</td>
<td>OS Selection: Not applicable</td>
</tr>
<tr>
<td>Boot order: CD, C:, Floppy</td>
<td>Boot order: CD, C:, Floppy</td>
</tr>
<tr>
<td>Post F1 prompt: Delayed</td>
<td>Post F1 prompt: Delayed</td>
</tr>
<tr>
<td>Hyperthreading: Enabled</td>
<td>Hyperthreading: Enabled</td>
</tr>
</tbody>
</table>

Table 11: RAID Settings

<table>
<thead>
<tr>
<th>Cisco MCS 7825 (HP and IBM)</th>
<th>Cisco MCS 7835 (HP and IBM)</th>
<th>Cisco MCS 7845 (HP and IBM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID not applicable</td>
<td>Logical drives: 1</td>
<td>Logical drives: 2</td>
</tr>
<tr>
<td>Cisco MCS 7825 (HP and IBM)</td>
<td>Cisco MCS 7835 (HP and IBM)</td>
<td>Cisco MCS 7845 (HP and IBM)</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>RAID not applicable</td>
<td>RAID type: 1(1+0)</td>
<td>RAID type: 1(1+0)</td>
</tr>
</tbody>
</table>

**Note** For the Cisco 7825H1 and the Cisco 7825I1, SATA RAID is enabled, and the RAID type is 1(1+0), with one logical drive.

---

**Access Cisco Unified CM IM and Presence Administration**

Complete the following procedure to access the Cisco Unified CM IM and Presence Administration interface.

**Procedure**

**Step 1** Open a browser and enter https://<servernameorIPaddress>, where the server name or IP address equals the server where the IM and Presence Service is installed.

**Step 2** From Administrative Applications, select Cisco Unified Communications Manager IM and Presence.

**Step 3** If the system prompts you about certificates, you must enable HTTPS to secure communications between the browser client and the web server. See the *Release Notes for Cisco Unified Communications Manager* for more information about how to load the required certificates for the HTTPS connection.

**Step 4** Enter the application username and application user password that you specified during installation when the system prompts you for a user name and password. The Cisco Unified CM IM and Presence Administration interface displays.

**Step 5** To access other IM and Presence interfaces, select an interface from the Navigation drop-down list and select Go.