



Installation Guide for Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1)

First Published: 2016-06-07

Last Modified: 2021-04-22

Americas Headquarters

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	vii
Purpose	vii
Audience	vii
Related Documentation	vii
Conventions	viii
Obtain Support	x
Cisco Product Security Overview	x

CHAPTER 1

Getting started	1
About Cisco Unified Communications Manager	1
About the IM and Presence Service	1
About the System Topology	1

CHAPTER 2

Installation Planning	3
Requirements and Limitations	3
Limitations	3
Subnet Limitations	3
Cluster Size	4
Network Requirements	4
IP Address Requirements	4
DNS requirements	4
Firewall Requirements	5
Platform Requirements	5
Software Requirements	5
Version Requirements	5
Software Restrictions	8

- Browser Requirements 8
- User Name and Password Requirements 9
 - Accounts and Passwords for Unified Communications Manager 9
 - Accounts and Passwords for IM and Presence Service 11
 - Password Recommendations 11
- Installation Time Requirements 12
- Licensing Requirements 12
 - Cisco Unified Communications Manager License Requirements 12
 - IM and Presence license requirements 12
- Required Installation Information 13
- Export Restricted and Export Unrestricted Software 18

CHAPTER 3

Installation Overview 21

- Installation Overview 21
 - Types of Installation 21
- Installation and Configuration Task Lists 22
 - Perform a Basic Installation 23
 - Apply a Patch to Upgrade During an Installation 23
 - Install a New Node in an Existing Cluster 24
 - Configure a Server with Pre-Installed Software 25
 - Perform an Unattended Installation 25
 - Install a Unified Communications Manager Cluster in Parallel 26
 - Install an IM and Presence Service Cluster 27

CHAPTER 4

Pre-Installation Tasks 29

- Perform Pre-Installation Tasks for Unified Communications Manager Nodes 29
- Perform pre-installation tasks for IM and Presence nodes 31
- Verify DNS Registration 32
- Generate answer file 32
- Reformat USB key to FAT32 file system 32

CHAPTER 5

Installation Tasks 35

- Before You Begin 35
 - Installation Wizard 35

Touchless Installation for Virtual Machine	36
Automatic Sequencing of Touchless Server	36
Answer File Generator	37
Predefined Cluster Configurations (AFG Process)	37
Touchless Installation Configuration Task Flow	37
Generate and Download a Floppy Image	38
Install a Cluster	39
IM and Presence Service Integration	41
Install Software	41
Start Basic Installation	41
Enter Preexisting Configuration Information	43
Apply a Patch to Upgrade During Installation	44
Upgrade From a Local Source	45
Upgrade From a Remote Server	45
Configure Installation	48
Configure Basic Installation	48
Set Up Unified Communications Manager Publisher Node	49
Set Up Subscriber Node	52



Preface

- [Purpose, on page vii](#)
- [Audience, on page vii](#)
- [Related Documentation, on page vii](#)
- [Conventions, on page viii](#)
- [Obtain Support, on page x](#)
- [Cisco Product Security Overview, on page x](#)

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.

Related Documentation

For additional installation and upgrade information, refer to the following documents:

- *Cisco Prime Collaboration Deployment Administration Guide*

This document describes how to use the Cisco Prime Collaboration Deployment application, which is designed to assist in the management of Unified Communication applications. You can use this application to perform tasks such as migrate existing clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

- *Upgrade Guide for Cisco Unified Communications Manager*

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

This document describes how to upgrade Cisco Unified Communications Manager.

- *Administration Guide for Cisco Unified Communications Manager*

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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*

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

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*

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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:

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html.

The following table lists URLs for software and additional documentation.

Table 1: Quick Reference for URLs

Related Information and Software	URL
Cisco Unified Communications Manager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
italic font	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font .
boldface screen font	Information you must enter is in boldface screen font .
italic screen font	Arguments for which you supply values are in italic screen font.
^	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 Dkey.
◊	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:



Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:



Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:



Tip Means the information contains useful tips.

Cautions use the following conventions:



Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtain Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Ciscodocuments, see the monthly What'sNew in CiscoProduct Documentation, which also lists all new and revised Ciscotechnical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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.



CHAPTER 1

Getting Started

The following sections provide information about Cisco Unified Communications Manager and the IM and Presence Service, and the relationship between these nodes when they are installed together in a cluster.

- [About Cisco Unified Communications Manager, on page 1](#)
- [About the IM and Presence Service, on page 1](#)
- [About the System Topology, on page 1](#)

About Cisco Unified Communications Manager

Cisco Unified Communications Manager serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Unified Computing System (UCS) servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

About the IM and Presence Service

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 availability 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.

About the System Topology

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

Clusters

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

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

Publisher Nodes and Subscriber Nodes

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

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

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



CHAPTER 2

Installation Planning

The following sections provide information about the installation requirements.

- [Requirements and Limitations, on page 3](#)
- [Licensing Requirements, on page 12](#)
- [Required Installation Information, on page 13](#)
- [Export Restricted and Export Unrestricted Software, on page 18](#)

Requirements and Limitations

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



Caution

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

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

Limitations

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

Subnet Limitations

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

Cluster Size

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

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

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

Network Requirements

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

IP Address Requirements

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

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

DNS requirements

Note the following requirements:

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

Firewall Requirements

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

Platform Requirements

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

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

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

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

Software Requirements

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

Version Requirements

For 11.x Versions up to 11.5(1)SU1

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first three numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 11.0.1.10000-1 is compatible with Unified Communications Manager software version 11.0.1.30000-2. Refer to the following table for sample Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.

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

Sample Unified Communications Manager Version	Example of Compatible IM and Presence Service Version
11.0.1.30000-2	11.0.1.10000-1
11.5.1.10000-6	11.5.1.10000-4

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must also be 11.5.1.10000-1.

Release 11.5(1)SU2

For Release 11.5(1)SU2, both Unified Communications Manager and IM and Presence Service must be running official 11.5(1)SU2 versions. Running an 11.5(1)SU2 version of Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU2 version of IM and Presence Service with an earlier version of Unified Communications Manager is not supported.

The following software versions are supported with Release 11.5(1)SU2:

- Unified Communications Manager 11.5.1.12900-21
- IM and Presence Service 11.5.1.12900-25

Release 11.5(1)SU3

For Release 11.5(1)SU3, both Unified Communications Manager and IM and Presence Service must be running official 11.5(1)SU3 versions. Running an 11.5(1)SU3 version of Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU3 version of IM and Presence Service with an earlier version of Unified Communications Manager is not supported.

The following software versions are supported with Release 11.5(1)SU3:

- Unified Communications Manager 11.5.1.13900-52
- Unified Communications Manager 11.5.1.13901-3
- Unified Communications Manager 11.5.1.13902-2
- IM and Presence Service 11.5.1.13900-57
- IM and Presence Service 11.5.1.13901-1

Release 11.5(1)SU4

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.14900-11
- IM and Presence Service 11.5.1.14900-32

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

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU4 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU4 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU4 version.

Release 11.5(1)SU5

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.15900-18

- IM and Presence Service 11.5.1.15900-33

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

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU5 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU5 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU5 version.

Release 11.5(1)SU6

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.16900-16
- IM and Presence Service 11.5.1.16910-12

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

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU6 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU6 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU6 version.

Release 11.5(1)SU7

The following versions are supported:

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

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

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

Release 11.5(1)SU8

The following versions are supported:

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

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

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

Software Restrictions

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

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

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

Browser Requirements

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

Table 3: Supported Browsers and Operating Systems

You can use this browser...	...with one of these operating systems
Google Chrome (latest browser version)	Microsoft Windows 10 (64 bit)
Microsoft Internet Explorer 11	<ul style="list-style-type: none"> • Microsoft Windows 10 (64 bit) • Microsoft Windows 8.1 (64 bit) • Microsoft Windows 7 (64 bit)
Microsoft Edge	Microsoft Windows 10 (32 bit/64 bit)
Mozilla Firefox (latest browser version)	Microsoft Windows 10 (64 bit)
Safari	Apple Mac OS 10.x (or newest OS release available)

User Name and Password Requirements

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

Accounts and Passwords for Unified Communications Manager

User Name and Password Requirements



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

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

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

Administrator Account User Name and Password

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

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

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

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

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

Application User Name and Password

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

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

- Cisco Unified Reporting

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

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

**Caution**

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

System application names are:

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

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

Security Password

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

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

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

If your security password is less than 14 characters:

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

Accounts and Passwords for IM and Presence Service

Required passwords

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

Administrator account username and password

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

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

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

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

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

Application username and password

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

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

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

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



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

Password Recommendations

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

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include special symbols.

- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

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

Installation Time Requirements

Time Requirements for Unified Communications Manager

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

Time Requirements for IM and Presence Nodes

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

Licensing Requirements

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

Cisco Unified Communications Manager License Requirements

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



Important

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

IM and Presence license requirements

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



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

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

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

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

For more information, see [System Configuration Guide for Cisco Unified Communications Manager](#).

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

Required Installation Information

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

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



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

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

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

Table 4: Required Installation Information

Configuration data	Description	Editable after installation
Administrator Credentials		
Administrator Login	Specifies the name that you want to assign to the Administrator account.	No After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password	Specifies the password for the Administrator account.	Yes CLI: <code>set password user admin</code>
Application User Credentials		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: <code>utils</code> <code>reset_application_ui_administrator_name</code>
Application User Password	Specifies the password for applications on the system.	Yes CLI: <code>utils</code> <code>reset_application_ui_administrator_password</code>
Security Password		
Security password for Unified Communications Manager	Servers in the cluster use the security password to communicate with one another. Set this password on the Unified Communications Manager publisher node, and enter it when you install each additional node in the cluster, including IM and Presence nodes.	Yes. You can change the security password on all nodes in the cluster using the following command: CLI: <code>set password user security</code>
Certificate Information		
Organization	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
Unit	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>

Configuration data	Description	Editable after installation
Location	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
State	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code>
Country	Used to create the Certificate Signing Request.	Yes CLI: <code>set web-security [orgunit] [orgname] [locality] [state]</code>
(Optional) SMTP		
SMTP Location	Specifies the name of the SMTP host that is used for outbound email. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.	Yes <ul style="list-style-type: none"> • In Cisco Unified Communications Operating System Administration: select Settings > SMTP and enter the IP address or Hostname in the SMTP Host Field. • CLI: <code>set smtp [host]</code>
NIC Interface Settings		
NIC Speed	If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) speed, you must select the NIC speed (either 10 megabit or 100 megabit).	Yes CLI: <code>set network nic eth0 {auto {en dis}} {speed {10 100}} {duplex half {half full}}</code> Note 1000BASE-T can only be enabled via auto-negotiation. Note Virtual machines do not support this command.
NIC Duplex	If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) duplex setting, you must select the NIC duplex setting (either Full or Half).	Yes CLI: <code>set network nic eth0 {auto {en dis}} {speed {10 100}} {duplex half {half full}}</code> Note 1000BASE-T can only be enabled via auto-negotiation. Note Virtual machines do not support this command.

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

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

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

Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and IM and Presence Service supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.



Note Unrestricted versions of software are intended only for a very specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.
- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.
- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.
- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and IM and Presence Service in the same cluster must either all be in unrestricted mode or all be in restricted mode.

- IP phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).



Note Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

For all Graphical User Interfaces (GUIs) and Command Line Interfaces (CLIs), the Administrator can view the product version (restricted or export unrestricted).

The following table describes the GUI items that are not available for the export unrestricted version of Unified Communications Manager and IM and Presence Service.

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

GUI Item	Location	Description
SIP Federated Domains	Presence > Inter-domain Federation > SIP Federation	When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode.
XMPP Federation Settings	Presence > Inter-domain Federation > XMPP Federation > Settings	You cannot configure the security mode; It is set to NO TLS .
Proxy Configuration Settings	Presence > Routing > Settings	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.



CHAPTER 3

Installation Overview

- [Installation Overview, on page 21](#)
- [Installation and Configuration Task Lists, on page 22](#)

Installation Overview

You can use the procedures in this section to install both the Cisco Unified Communications Manager and the IM and Presence Service.

If you are installing both Cisco Unified Communications Manager and IM and Presence Service nodes in your cluster, you must complete the installation and configuration tasks in the following order:

1. Install the Cisco Unified Communications Manager software on the first node and configure it as the publisher node for the cluster.
2. Install the Cisco Unified Communications Manager software on the subscriber nodes and configure them.
3. Perform all post-installation tasks for Cisco Unified Communications Manager nodes.
4. Install the IM and Presence Service and configure the node as the IM and Presence Service database publisher node.
5. Install the IM and Presence Service on the subscriber nodes and configure them.
6. Perform all post-installation tasks for the IM and Presence Service nodes.

Types of Installation

You can perform a basic installation, or you can upgrade during an installation. The table below describes these two options.

Table 5: Installation Types

Installation Types	Description
Basic installation	<p>This option represents the basic Cisco Unified Communications Manager installation, which installs the software from the installation disc or from an ISO file stored in a virtual machine. This option does not use any imported data.</p> <p>You can use this option to install the software manually, or you can use an answer generator file to perform an unattended installation.</p> <p>You can also use this option when you have a server on which the software is pre-installed.</p>
Apply a patch to upgrade during an installation (available on Unified Communications Manager nodes only)	<p>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.</p> <p>Note Ensure that you have the software image available on DVD or on a remote server prior to choosing this option.</p>

**Important**

- Install the software during off-peak hours or during a maintenance window to avoid impact from interruptions.
- 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 may be lost. 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.

Installation and Configuration Task Lists

The following sections provide a list of the high-level tasks that you must perform for each of the installation scenarios. For detailed information about how to perform these tasks, refer to the list of Related Topics included with each task list.

**Note**

For information about replacing a Unified Communications Manager server or cluster, or for information about changing the specifications of a virtual machine, refer to *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.

Perform a Basic Installation

Complete the high-level tasks listed in this section when you perform a basic installation on a Cisco Unified Communications Manager publisher node, or on a subscriber node in the cluster. Subscriber nodes can be either Cisco Unified Communications Manager nodes, or IM and Presence nodes.

Procedure

- Step 1** Perform all pre-installation tasks that apply to your site.
 - Step 2** Follow the procedure to start installing the software for a basic installation.
 - Step 3** Follow the procedure for configuring a basic installation.
 - Step 4** When the Configuration window displays, specify whether the server is the first node in the cluster (the publisher node), or a subscriber node:
 - choose **Yes** to configure the new server as the Cisco Unified Communications Manager publisher node
 - choose **No** to configure the new server as a subscriber node
 - Step 5** Follow the procedure to set up the node. Use the procedure for setting up the publisher node, or for setting up subscriber nodes, depending on the option that you chose in the previous step.
 - Step 6** Perform all post-installation tasks that apply to your site.
-

Apply a Patch to Upgrade During an Installation

Complete the high-level tasks listed in this section when you apply a patch and upgrade to a newer version of Unified Communications Manager during an installation. This option is available only for Unified Communications Manager nodes.

You can upgrade to a later release by downloading and applying a patch during installation of the Unified Communications Manager publisher node.

When you upgrade during an installation, the software versions must have the same major and minor release number. Major and minor release numbers are defined as follows:

10.x

where 10 = major release number and x = minor release number

Procedure

- Step 1** Perform all pre-installation tasks that apply to your site.
- Step 2** Follow the procedure to start installing the software for a basic installation.
- Step 3** Follow the procedure to apply a software patch.
- Step 4** Follow the procedure for configuring a basic installation.
- Step 5** When the Configuration window displays, specify whether the server is the first node in the cluster (the publisher node), or a subscriber node:
 - choose **Yes** to configure the new server as the Cisco Unified Communications Manager publisher node

- choose **No** to configure the new server as a subscriber node

- Step 6** Follow the procedure to set up the node. Use the procedure for setting up the first node, or for setting up subscriber nodes, depending on the option that you chose in the previous step.
- Step 7** Perform all post-installation tasks that apply to your site.
-

Install a New Node in an Existing Cluster

Complete the high-level tasks listed in this section when you install a new Cisco Unified Communications Manager node or a new IM and Presence node in an existing cluster. The new node must be a subscriber node and cannot be a Cisco Unified Communications Manager publisher node.



Note You must add an IM and Presence server using Cisco Unified CM Administration before installing the server node in a cluster. See topics related to adding a server before installing the node in the cluster in the *Administration Guide for Cisco Unified Communications Manager*.

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 as the publisher node. From Cisco Unified CM Administration on the publisher node, choose **System > Server** and configure the IP address for the subscriber 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 for a basic installation.
- You must install the same software version on all nodes in the cluster. If you do not have the correct version, you need to download updated software from Cisco.com.
- Step 7** Follow the procedure to configure the basic installation.
- Step 8** When the First Node Configuration displays, choose **No** to configure the new server as the subscriber node.
- Step 9** Follow the procedure for configuring a subscriber node.
- Step 10** Apply security to the new node in the cluster.
- Step 11** Perform all post-installation tasks that apply to your site.
- Step 12** 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 publisher node. After you finish installing the new node, you will need to update the CTL file on all nodes.

Note

- You can collect the logs from RTMT of a new node added to the existing FQDN cluster, only when you restart the trace collection service. When you sign in to Unified RTMT without restarting the trace collection, the following error message is displayed: Could not connect to 'Server' <new node name>.
- If you install a new node in an existing cluster where the IM and Presence server is not upgraded to the supported version or if the IM and Presence server has been decommissioned, the following error message is displayed: "Add failed. Upgrade and migration for Cisco Unified IM & Presence Servers that are associated with this cluster appears to be pending (not complete). Please make sure upgrade and migration of all IM & Presence servers is completed successfully before adding servers to this cluster. Please check for any unused IM & Presence Application Servers and delete them".

**Important**

After you install a new node in an existing cluster, all phones that are registered to the cluster are reset.

Configure a Server with Pre-Installed Software

Complete the high-level tasks listed in this section if you have a new server with either the Cisco Unified Communications Manager software or the IM and Presence software pre-installed. You must perform these tasks to configure the pre-installed software.

Procedure

- Step 1** Perform all pre-installation tasks that apply to your site.
- Step 2** Follow the procedure to start installing the software for a basic installation. When the Platform Installation Wizard window displays, choose **Skip**.
- Step 3** Follow the procedure to enter preexisting configuration information.
- Step 4** Follow the procedure for configuring a basic installation.
- Step 5** Perform all post-installation tasks that apply to your site.

Perform an Unattended Installation

Complete the high-level tasks listed in this section when you use the Cisco Unified Communications Answer File Generator to perform an unattended installation. This option is available only for fresh installations and is not supported if you are performing an upgrade during an installation. You can perform an unattended installation on either Cisco Unified Communications Manager nodes, or IM and Presence nodes.

Procedure

- Step 1** Perform all pre-installation tasks that apply to your site.
- Step 2** Ensure that a floppy image is mounted with an empty file that is named `POWER_OFF_AFTER_SKIP_INSTALL` before you begin the installation procedure.
- Step 3** Use the *Cisco Unified Communications Answer File Generator* to generate answer files.
- Step 4** Ensure that the USB key where you store the answer files has a FAT32 file system.
- Step 5** Follow the procedure to start installing the software for a basic installation.
- Step 6** Follow the procedure for configuring a basic installation.
- Step 7** When the **Configuration** window displays, specify whether the server is the publisher node in the cluster, or a subscriber node:
- Choose **Yes** to configure the new server as the Cisco Unified Communications Manager publisher node
 - Choose **No** to configure the new server as a subscriber node
- Step 8** Follow the procedure to set up the node. Use the procedure for setting up the publisher node, or for setting up subscriber nodes, depending on the option that you chose in the previous step.
- Step 9** Perform all post-installation tasks that apply to your site.
-

Install a Unified Communications Manager Cluster in Parallel

Complete the high-level tasks listed in this section to install Unified Communications Manager nodes in parallel. When you install nodes in parallel, you begin the installation of the publisher node and subscriber nodes at the same time.

Procedure

- Step 1** Perform all pre-installation tasks that apply to your site.
- Step 2** Follow the procedure to start installing the software for a basic installation. Begin the installation on all nodes.
- Step 3** Follow the procedure for configuring a basic installation.
- Step 4** When the **Configuration** window displays, designate one node to be the first node (the publisher node) and designate the remaining nodes as subscriber nodes:
- a) choose **Yes** to configure one node as the Cisco Unified Communications Manager publisher node
 - b) choose **No** on the remaining nodes to configure them as subscriber nodes

Do not proceed further with the installation of the subscriber nodes at this point. You must wait until you complete the installation of the publisher node before you continue with the installation of the subscriber nodes.
- Step 5** Follow the procedure for setting up a Unified Communications Manager publisher node.
- Step 6** Associate each of the subscriber nodes in the cluster with the publisher node using the Cisco Unified CM Administration interface. For more information, see the Administration Guide for Cisco Unified Communications Manager .
- Step 7** Follow the procedure to set up a subscriber node.

- Step 8** Perform all post-installation tasks that apply to your site.
-

Install an IM and Presence Service Cluster

Follow this sequence of tasks when you are configuring your multi-node IM and Presence Service deployment. You configure the IM and Presence Service multi-node feature, and manage your clusters, nodes and users using Cisco Unified CM Administration.

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

Before you begin

- Determine the type of multi-node deployment model that you are going to configure.
- The Cisco XCP Router must be running for all availability services to function properly on IM and Presence Service (both SIP-based and XMPP-based client messaging).

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 Service database node (the first server in the IM and Presence Service cluster).
- Note** Complete the installation of the IM and Presence Service database publisher node and confirm that services are running before you begin to install IM and Presence Service subscriber nodes.
- Step 3** (On the Cisco Unified Communications Manager publisher node) Create all presence redundancy groups and nodes in the cluster.
- Note** Do not add a node in the Cisco Unified Communications Manager server list during the installation process.
- Step 4** (On the IM and Presence Service database node) Associate each of the subscriber nodes in the cluster with the publisher node. You must associate the subscriber node with the publisher node before you install that subscriber IM and Presence Service node.
- Step 5** Install and configure each of the subscriber nodes in the cluster.
- Step 6** (On the Cisco Unified Communications Manager publisher node) Assign these nodes to the appropriate presence redundancy group.

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

Note Before you assign or move a node to a presence redundancy group, check the following:

- From the System troubleshooter page, verify that the Cisco IM and Presence Data Monitor 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 Service services are running.
- If you plan to move or unassign a node in a presence redundancy group, you must turn off high-availability in that presence redundancy group before you move or unassign the node.

- Step 7** Turn on high-availability in the presence redundancy group as required. See the *Administration Guide for 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 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

- If you assign a node before you start the IM and Presence Service 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 Service services, select **Cisco Unified Serviceability > Tools > Control Center - Network Services**.
- The Cisco IM and Presence Data Monitor service delays feature service startup on subscriber nodes if IDS replication is not successfully established.



CHAPTER 4

Pre-Installation Tasks

- [Perform Pre-Installation Tasks for Unified Communications Manager Nodes, on page 29](#)
- [Perform pre-installation tasks for IM and Presence nodes, on page 31](#)
- [Verify DNS Registration, on page 32](#)
- [Generate answer file, on page 32](#)
- [Reformat USB key to FAT32 file system, on page 32](#)

Perform Pre-Installation Tasks for Unified Communications Manager Nodes

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

Procedure

- Step 1** Review the installation requirements and record the configurations settings for each server that you plan to install.
- Step 2** For every node in your cluster, create virtual machines using the Virtual Server Template (OVA file) recommended for your current release.
- Different OVA files are available; choose the correct OVA file based on the environment in which you are deploying Unified Communications Manager.
- Step 3** Place the installation ISO file in a location where the virtual machine can access it and edit the virtual machine's DVD drive to map to the file. Select the option to mount the DVD drive when you power on the virtual machine.
- When you power on the virtual machine, it will mount the ISO file and start the installation process. Do not begin the installation process until you have completed all of the steps in this procedure.
- Step 4** If you are installing a cluster or adding a 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 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 publisher node can synchronize with the NTP server before you install a subscriber node. Log into the Command Line Interface on the publisher 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 publisher node fails to synchronize with an NTP server, installation of a subscriber node can also fail.
- Note** Ensure that the VMware ESXi software underneath the Cisco Unified Communications Manager is using the same NTP server as the Cisco Unified Communications Manager application or NTP servers having the same Stratum. See VMware documentation for more information.
- Step 6** If your firewall is 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 servers where you are installing Unified Communications Manager.
- Step 8** Ensure that the network interface card (NIC) speed and duplex settings on the switch port are the same as those that you plan to set on the new server.
- For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.
- Step 9** 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 10** If you use DNS, verify that all servers on which you plan to install Unified Communications Manager are properly registered in DNS.
- Step 11** If you are using a server that is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi.
- Boot the server and press F2 when prompted during bootup.
 - Select **Advanced** tab.
 - Select **Mass Storage Controllers Configuration**.
 - Set the Onboard SATA Controller to **Disabled**.
- Step 12** Obtain a license file.
- Note** For more information on specifying the required number of licenses, refer to the *Administration Guide for Cisco Unified Communications Manager*.
- Step 13** Configure any subscriber nodes on the publisher node before you install a subscriber node.

From Cisco Unified CM Administration on the publisher node, choose **System > Server** and configure the IP address for the subscriber nodes. For more information, see the *Administration Guide for Cisco Unified Communications Manager*.

Perform pre-installation tasks for IM and Presence nodes

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

Procedure

- Step 1** Ensure that the Unified Communications Manager and IM and Presence software versions are compatible.
- Step 2** Gather all the information you need to complete the installation and configuration of the IM and Presence software.
- Step 3** For every node in your cluster, create virtual machines using the Virtual Server Template (OVA file) recommended for your current release.
- Different OVA files are available; choose the correct OVA file based on the environment in which you are deploying Unified Communications Manager.
- Step 4** Configure subscriber nodes on the publisher node before you install a subscriber node.
- From Cisco Unified CM Administration on the publisher node, choose **System > Server** and configure the IP address for the subscriber nodes. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
- Step 5** Ensure that the IM and Presence server has network access to the Unified Communications Manager publisher server.
- You can ping Unified Communications Manager from other servers.
- Step 6** Ensure that you turn on the Cisco AXL Web Service on the associated Unified Communications Manager server.
- Select **Tools > Service Activation** in Cisco Unified Serviceability.
- Step 7** If you use DNS, ensure that you have configured the hostname of the new IM and Presence server on the DNS server and that the DNS server can resolve the hostname of the Unified Communications Manager publisher server and of other IM and Presence servers (if any).
- Caution** Cisco recommends that you use the same DNS servers between IM and Presence and Unified Communications Manager. If you use different DNS servers, it is likely to cause abnormal system behavior. Both Unified Communications Manager and IM and Presence must either use or not use DNS because Cisco does not support mixed-mode deployments. If you are using the multinode feature in IM and Presence, see the *Deployment Guide for IM and Presence Service on Unified Communications Manager* for DNS configuration options.
-

Verify DNS Registration

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

Procedure

- Step 1** Open a command prompt.
 - Step 2** To ping each server by its DNS name, enter ping DNS_name.
 - Step 3** To look up each server by IP address, enter nslookup IP_address.
-

Generate answer file

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

Before you begin

Gather the required installation and configuration information.

Procedure

- Step 1** Access the CiscoUnified 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 subscriber 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.
-

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.
-



CHAPTER 5

Installation Tasks

- [Before You Begin, on page 35](#)
- [Touchless Installation for Virtual Machine, on page 36](#)
- [Install Software, on page 41](#)
- [Apply a Patch to Upgrade During Installation, on page 44](#)
- [Configure Installation, on page 48](#)

Before You Begin

Before you begin the installation, review the following information:

- Make sure that the subscriber nodes that you are installing can connect to the publisher node server during the installation.
- Make sure that all Cisco Unified Communications Manager servers in a cluster have the same software version. Make sure that all IM and Presence servers in a cluster have the same version of the released software. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed. If you are installing IM and Presence nodes, Cisco Unified Communications Manager and IM and Presence Service software versions must have the same major and minor release number.
- Do not attempt to perform any configuration tasks during the installation.
- Be aware that directory names and filenames that you enter while you are running the installation program are case-sensitive.
- For 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 reset. Examples of phone user settings includes 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.

Installation Wizard

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

Table 6: Installation Wizard Navigation

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



Note The installation wizard supports the following characters:

- alphanumeric: A-Z, a-z, and 0-9- spaces
- spaces and # (except as the first character)
- only the following special characters: \, - _ ; { } () []

all other characters are not supported.

Touchless Installation for Virtual Machine

Previous releases of Cisco Unified Communications Manager cluster environment required you to install the publisher node first before you proceed to install the subscriber nodes. You had to install the subscriber nodes after adding them to the server page of the publisher node and repeat the same procedure for each subscriber node. With the touchless installation feature, the subscriber nodes are configured dynamically along with the publisher node during their installation.

Touchless installation is a new feature in Cisco Unified Communications Manager. This feature makes the installation process seamless and promotes simplified cluster installation. The touchless installation proceeds without the requirement to provide any subscriber details in the installation wizard. Subscribers are not dependent on the installation of the publisher. This feature has the following benefits:

- No manual intervention and scheduling during the deployment of a new cluster.
- No manual entry of each subscriber and simplifies the addition of new subscribers to an existing cluster.
- No requirement to wait until the publisher node is active.

Automatic Sequencing of Touchless Server

Automatic sequencing is an approach that facilitates the installations of both the publisher node and the subscriber nodes in a cluster at the same time without manual intervention. Subscriber nodes wait for the publisher node to complete its installation, and then get added to the database of the publisher node to continue

with their own installation. After the publisher node is installed, it authenticates each subscriber. After authentication, each subscriber node receives a signal from the publisher node and the installation of that subscriber node continues automatically.

Initiate automatic sequencing by enabling the **Dynamic Cluster Config Enable** timer checkbox and providing a value in the **Dynamic Cluster Config Timer** field. You can enable this timer by using one of the following methods:

- Answer File Generator (AFG) tool.
- Command line interface (CLI) command on the Cisco Unified Communications Manager publisher node.

Answer File Generator

Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to generate the answer files or floppy image files for configuration. These files include `clusterConfig.xml` and `platformConfig.xml` files. The `clusterConfig.xml` file is a new file in Cisco Unified Communications Manager Release 10.5(2).

Start the virtual machine on which you mounted the ISO and floppy image to start the Cisco Unified Communications Manager installation. No manual intervention is required during installation of a standalone node or a cluster.

In a cluster environment, you can install both the publisher node and the subscriber nodes simultaneously. Sometimes, the installation of the subscriber nodes can stop during the installation of the publisher node. In this case, after the publisher node installation is complete, it generates a signal for the subscriber nodes to continue their installation.

Predefined Cluster Configurations (AFG Process)

With the implementation of this feature, the Answer File Generator (AFG) tool generates the `clusterConfig.xml` file along with the existing the `platformConfig.xml` file. If you provide the details of subscriber nodes to the AFG tool, the `clusterConfig.xml` file includes those details. After the Cisco Unified Communications Manager publisher is installed, it reads the `clusterConfig.xml` file and if the publisher finds any subscriber nodes, it adds them to its processnode tables. Adding the subscribers to processnode tables eliminates the need to wait for the Cisco Unified Communications Manager publisher to finish its installation, and then manually add the subscribers on the server page. The entire installation process occurs automatically.

Touchless Installation Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate and Download a Floppy Image, on page 38.	Generate the floppy image using the Answer File Generator tool. The floppy image consists of two precreated answer files— <code>platformConfig.xml</code> and <code>ClusterConfig.xml</code> files that are downloaded automatically when you download the floppy image.

	Command or Action	Purpose
Step 2	<p>Install a Cluster, on page 39</p> <ul style="list-style-type: none"> • Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 39 • Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 39 	<p>Install a cluster in one of the following ways:</p> <ul style="list-style-type: none"> • Install the publisher node and subscriber nodes with no manual intervention by enabling the Dynamic Cluster Config Enable timer. • Install the subscriber nodes when you do not enable the Dynamic Cluster Config Enable timer while generating the answer files.

Generate and Download a Floppy Image

The Cisco Unified Communications Answer File Generator web application generates the answer files for Cisco Unified Communications installations. These precreated answer files are `platformConfig.xml` and `ClusterConfig.xml` files and are included in the floppy image.

Perform the following procedure to generate and download the floppy image:

Procedure

-
- Step 1** Log in to the Cisco Unified Communications Answer File Generator application.
- Step 2** Enter details in the **Clusterwide Configuration** section.
- Step 3** Enter details for the primary node in the **Primary Node Configuration** section.
- Step 4** To enable Dynamic Cluster Configuration, from the **Dynamic-Cluster-Configuration** section, enable the **Dynamic Cluster Config Enable** timer check box and enter a value in the **Dynamic Cluster Config Timer** field.
- Specify a value from 1 to 24 for this field, where the number indicates hours.
- Note** If you do not enable the **Dynamic Cluster Config Enable** timer and specify its value in the **Dynamic Cluster Config Timer** field while you to generate the answer files, you will have to enable this timer later when the publisher node gets installed automatically but the subscriber nodes are waiting for installation. Then, you will have to add the subscriber nodes manually so that their installation occurs automatically.
- Step 5** Enter details for the secondary node in the **Secondary Node Configuration** section.
- Step 6** In the **List of Secondary Nodes** list box, select **Add Secondary Node**.
The node that you add as secondary node appears in this list box.
- Step 7** Repeat Steps 5 and 6 for additional secondary nodes.
- Step 8** Click **Generate Answer Files**.
A dialog box appears showing the details for the primary node, the secondary node, and the `clusterConfig` file.
- Step 9** In the **Communications Answer File Generator** dialog box, follow the download instructions, and then click the **Download File** button to download the answer files to your computer.
-

Install a Cluster

Depending on whether you enabled the **Dynamic Cluster Config Enable** timer in the Answer File Generator tool or not, you can choose one of the following ways to install a cluster:

- Install the publisher node and subscriber nodes with no manual intervention by enabling the **Dynamic Cluster Config Enable** timer. See [Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 39](#).
- Install the subscriber nodes when you do not enable the **Dynamic Cluster Config Enable** timer while generating the answer files. See [Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 39](#).

Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled

Before you begin

Enable the **Dynamic Cluster Config Timer** field by one of the following ways:

- Click the **Dynamic Cluster Config Enable** timer checkbox and enter a value in the **Dynamic Cluster Config Timer** field in the Answer File Generator tool. For details, see Step 4 of the [Generate and Download a Floppy Image, on page 38](#) procedure.
- Enter the **set network cluster subscriber dynamic-cluster-configuration** *{default | no. of hours}* CLI command.

Procedure

Step 1 Mount the floppy image on the virtual machine.

Note If the virtual machine is Cisco Unified Communications Manager publisher node, then the floppy image contains both the `platformConfig.xml` and `ClusterConfig.xml` files. However, if the virtual machine is Cisco Unified Communications Manager subscriber node or IM and Presence publisher node or subscriber nodes, the floppy image contains only the `platformConfig.xml` file.

For details on how to create a floppy a new virtual floppy image, see http://docwiki.cisco.com/wiki/How_to_Use_the_AFG_with_the_Virtual_Floppy_Drive.

Step 2 Start the publisher node and all subscriber nodes. Publisher node and subscriber nodes get installed automatically with no manual intervention. Each subscriber node gets automatically added to the publisher through the automatic sequencing approach.

Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled

If you do not enable the **Dynamic Cluster Config Timer** field in the Answer File Generator tool, the publisher node gets installed automatically. However, the subscriber nodes will be waiting for their installation.

To avoid the waiting time of the subscriber nodes so that the cluster installation continues, perform one of following tasks:

- From the Cisco Unified Communications Manager, select the **Web Interface** and click the **Server** tab and add the subscriber nodes manually.
- Enable the **Dynamic Cluster Config Timer** field from the CLI of the publisher node with the new CLI command that is available in Cisco Unified Communications Manager Release 10.5(2)—**set network cluster subscriber dynamic-cluster-configuration** {*default* | *no. of hours*}. After you enable this timer, the subscriber nodes get added to the publisher automatically and the installation of the subscriber nodes proceeds.

**Note**

- If you need to add one or more subscribers as specified for the publisher node, you can add them while you generate the `platformconfig.xml` file. You have to specify the publisher node and the subscriber nodes. If the **Dynamic Cluster Config Timer** timer is still active, subscribers get automatically added to the publisher and the installation of the subscriber nodes continues.
- This feature has no limitation on predefining the number of subscriber nodes that you need to add to a publisher node.

Use the WinImage tool to create the disk images. Mount the ISO images through VMware ESXi.

Before you begin

Place the floppy image at datastore from where it is accessible to virtual machine for mounting.

Procedure

-
- Step 1** Start the virtual machine to start the cluster installation.
- Step 2** From the **VM** menu, choose **Edit settings** to mount the floppy image that you have created from the Answer File Generator tool.
The **Virtual Machine Properties** dialog box appears.
- Step 3** From the available hardware list, select **Floppy drive 1**.
- Step 4** In the **Device Type** section, select **Use the existing floppy image in the database**, and then click **Browse** to navigate to the floppy image.
- Step 5** Click **OK**.
The floppy image is attached.
- Step 6** Select the **CD/DVD Drive 1 > Connect to ISO image on local disk** option from the toolbar and choose **CD/DVD Drive1 > Connect to ISO image on a datastore**, navigate to the data store to select the installer ISO image, and click **OK**.
The ISO image is attached and the installation starts.
- Step 7** (Optional) If you want to test the media before the installation, click **OK** in the **Disc Found** message box, or click **Skip** to skip testing the media before the installation.
The installation proceeds without any manual intervention. The publisher is installed and the subscribers are added to the publisher.
-

IM and Presence Service Integration

This feature supports heterogeneous cluster-wide installation that includes Cisco Unified Communications Manager and IM and Presence Service nodes. The concept and installation process for IM and Presence Service is same as the installation process for Cisco Unified Communications Manager in a cluster.

From the AFG tool, check the **Dynamic Cluster Config Timer** check box, select IM and Presence Service, and enter the details for Cisco Unified Communications Manager publisher node, IM and Presence Service publisher node, and IM and Presence Service subscriber details (if any). Then, AFG tool generates the `clusterConfig.xml` file along with `platformConfig.xml` file for each node. You can use this `clusterConfig.xml` file only with Cisco Unified Communications Manager publisher node along with `platformConfig.xml` file that is generated for this node. For all other nodes, only `platformConfig.xml` file is used.

Answer File Generator (AFG) saves the domain name of IM and Presence Service publisher in the `clusterConfig.xml` file along with the existing details.

The integration of Cisco Unified Communications Manager with IM and Presence includes the following tasks:

- The IM and Presence Service publisher is added to the `processnode` table with domain name after the installation of Cisco Unified Communications Manager.
- Cisco Unified Communications Manager and IM and Presence Service nodes are added to the `processnode` table using the IP address, if available.
- When you add the IM and Presence Service publisher through CLI, the domain is added.

Install Software

Use the procedures in this section to begin the software installation.

Start Basic Installation

To start the installation, follow this procedure.



Note If you are installing a subscriber node or adding a node to an existing cluster, you must configure the hostname or IP address of the new node on the publisher node in the cluster. From Cisco Unified CM Administration on the publisher node, choose **System > Server** and enter the IP address or hostname of the subscriber node. For more information, see the *Cisco Unified Communications Manager Administration Guide*.



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

Procedure

- Step 1** If you are using a configuration file created by the Answer File Generator, ensure that the file is accessible to the system:
- insert the USB key with the configuration information now
 - place the virtual floppy image in a location where the virtual machine can access it
- Note** If you have a new server with the software pre-installed, you do not need to install from a DVD or ISO file, unless you want to re-image the server with a later product release. Go directly to the configure basic installation procedure to enter the configuration information; see the Related Topics below for more information.
- Step 2** Perform one of the following actions:
- If you are installing from a DVD drive a VMware ESXi server host, insert the installation DVD into the tray and restart the server, so that it boots from the DVD.
 - If you are installing from a data store ISO file located on the local ESXi host or on a storage area network (SAN), edit the CD/DVD drive on the virtual machine to select the data store ISO file. Select the option to connect at power on, and restart the virtual machine. If you configured the virtual machine to use the ISO at the same time that you created the virtual machine using the OVA file, skip this step and complete the rest of the procedure.
- After the server completes the boot sequence, the **DVD Found** window displays.
- Step 3** 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** In the **Product Deployment Selection** window, specify the product to install:
- If you are installing the IM and Presence Service, select **OK**.
 - If you are installing a Cisco Unified Communications Manager application, select the product to install and choose **OK**. You can choose from the following options:
 - Cisco Unified Communications Manager
 - Cisco Unity Connection
 - Cisco Prime 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 Cisco Prime License Manager is installed co-resident automatically as part of this installation. Following the installation, Cisco Prime License Manager can be used to provide simplified, enterprise-wide management of user-based licensing, including license fulfillment. Cisco Prime 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 *Cisco Prime License Manager User Guide*.

Step 6 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 or ISO file. 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 7 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 configure basic installation procedure to enter the configuration information.
 - Manually configure the software that is pre-installed on your server – In this case you do not need to install the software, but you must configure the pre-installed 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 pre-install 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 8 In the **Apply Additional Release** window, choose one of the following installation types:

- 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 or to install IM and Presence nodes, choose **No**.
- To return to the previous window, choose **Back**.

Step 9 In the **Basic Install** window, choose **Continue** to install the software or configure the pre-installed software. Perform the configure basic installation procedure to configure the basic installation.

Enter Preexisting Configuration Information

Follow this procedure if you have a server that has the product pre-installed, or if you installed the product earlier but chose **Skip** in the Platform Installation Wizard window to configure the server at a later time.

Procedure

- Step 1** After the system restarts, the **Preexisting Installation Configuration** window displays.
- Step 2** If you have preexisting configuration information that the Answer File Generator created, that is stored on a USB key, insert the USB key 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** In the **Apply Additional Release** window, choose one of the following installation types:
- 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**. Perform the configure basic installation procedure to configure the basic installation.
-

Apply a Patch to Upgrade During Installation

This option is available when you install Unified Communications Manager nodes. It is not available for IM and Presence nodes.

If you choose **Yes** in the Apply a Patch window, the installation wizard installs the software version that is on the DVD or ISO image 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.
-

For information about supported upgrades, see the Release Notes for your product release and the Cisco Unified Communications Manager Compatibility Matrix at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html.

You can access the upgrade file during the installation process from an ISO image on a data store, 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 procedure to upgrade from a remote server..
 - FTP - Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the procedure to upgrade from a remote server.
 - LOCAL - Retrieves the upgrade file from a local DVD or from an ISO image on a data store. Continue with the procedure to upgrade from a local disk.
-

Upgrade From a Local Source

Before you can upgrade from a local source, you must download the appropriate patch file from Cisco.com. You must create an ISO image from the upgrade file and then either place it on a DVD or in the DVD drive of a virtual machine.

Procedure

- Step 1** When the **Local Patch Configuration** window displays, enter the patch directory and patch name, if required, and choose **OK**.
The **Install Upgrade Patch Selection Validation** window displays.
- Step 2** The window displays the patch file. To update the system with this patch, click **Continue**.
- Step 3** Choose the upgrade patch to install. The system installs the patch, then restarts the system with the upgraded software version running.
After the system restarts, the **Preexisting Configuration Information** window displays.
- Step 4** To continue the installation, choose **Proceed**.
The **Platform Installation Wizard** window displays.
- Step 5** To continue the installation, click **Proceed** or click **Cancel** to stop the installation.
If you click **Proceed**, the **Apply Patch** window displays. Continue with the next step.
If you click **Cancel**, the system halts, and you can safely power down the server.
- Step 6** When the **Apply Patch** window displays, choose **No**.
- Step 7** The **Upgrade** window displays.
- Step 8** Click **No** and perform the procedure to configure the basic installation.
-

Upgrade From a Remote Server

Use this procedure to upgrade Unified Communications Manager nodes from a remote server. This option is not available for IM and Presence nodes.

Before you can upgrade Unified Communications Manager 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.

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** Configure the auto negotiation setting.
- To enable automatic negotiation, choose **Yes**. This option sets the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. The **MTU Configuration** window displays. Skip the next step then continue.
- Note** To use this option, your hub or Ethernet switch must support automatic negotiation.
- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays. Continue with the next step.
- Step 2** If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.
- The **MTU Configuration** window displays.
- Step 3** In the **MTU Configuration** window, you can change the MTU size from the operating system default.
- The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value.
- Caution** If you configure the MTU size incorrectly, your network performance can be affected.
- To accept the default value (1500 bytes), choose **No**.
 - To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.

The **DHCP Configuration** window displays.

- Step 4** For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.
- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The installation process attempts to verify network connectivity.
 - If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.
- Step 5** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. The **DNS Client Configuration** window displays.
- Step 6** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. After the system configures the network and checks for connectivity, the Remote Patch Configuration window displays.
- Step 7** Enter the location and login information for the remote file server. The system connects to the remote server and retrieves a list of available upgrade patches.
- If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter **/patches**
- If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including:
- Begin the path with a forward slash (/) and use forward slashes throughout the path.
 - The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).
- The **Install Upgrade Patch Selection** window displays.
- Step 8** Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system with the upgraded software version running.
- After the system restarts, the **Preexisting Configuration Information** window displays.
- Step 9** To continue the installation, choose **Proceed**. The **Platform Installation Wizard** window displays.
- Step 10** Choose **Proceed** or Choose **Cancel** to stop the installation.
- If you choose **Proceed**, the **Apply Patch** window displays. Continue with the next step.
- If you choose **Cancel**, the system halts, and you can safely power down the server.
- Step 11** In the **Apply Patch** window displays, choose **No**. The **Windows Upgrade** window displays.
- Step 12** Choose **No** and perform the configure basic installation procedure to configure the basic installation.
-

Configure Installation

Use the procedures in this section to configure the servers and complete the installation.

Configure Basic Installation

Procedure

- Step 1** In the **Timezone Configuration** window, choose the appropriate time zone for the server and then choose **OK**.
The **Auto Negotiation Configuration** window is displayed.
- Step 2** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.
- To enable automatic negotiation, choose **Yes**.
The **MTU Configuration window** is displayed.
Note To use this option, your hub or Ethernet switch must support automatic negotiation.
 - To disable automatic negotiation, choose **No** and continue with the next step.
The **NIC Speed and Duplex Configuration** window is displayed.
- Step 3** If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.
The **MTU Configuration** window displays.
- Step 4** In the **MTU Configuration** window, you can change the MTU size from the operating system default.
The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.
- Caution** If you configure the MTU size incorrectly, your network performance can be affected.
- To accept the default value (1500 bytes), choose **No**.
 - To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.
- The **DHCP Configuration** window displays.
- Step 5** For network configuration, you can choose to either set up a static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.
- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The network restarts, and the **Administrator Login Configuration** window is displayed.

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

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. The **DNS Client Configuration** window is displayed.

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

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

- **Proceed:**

- Click **Proceed** to restart the network using the new configuration. The **Administrator Login Configuration** window is displayed.
- Enter Administrator login **User Name** and **Password**

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

- **Software Location of Data to Import**

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

Step 9 The **Certificate Information** window is displayed.

Step 10 In **Certificate Information** window, enter your certificate signing request information and click **OK**.

Step 11 In the **First Node Configuration** window, choose how you want to assign this node:

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

Set Up Unified Communications Manager Publisher Node

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



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

Procedure

- Step 1** The **Network Time Protocol Client Configuration** window appears.
- Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher node. Subscriber nodes in the cluster will get their time from the first node.
- Step 2** Choose whether you want to configure an external NTP server or manually configure the system time.
- Note** Ensure that the VMware ESXi software underneath the Cisco Unified Communications Manager is using the same NTP server as the Cisco Unified Communications Manager application or NTP servers having the same Stratum. See VMware documentation for more information.
- 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 four, ideally five. Choose **Proceed** to continue with the installation.
- The system contacts an NTP server and automatically sets the time on the hardware clock.
- Note** If the **Test** button appears, you can choose **Test** to check whether the NTP servers are accessible.
- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.
- The **Database Access Security Configuration** window appears.
- Step 3** Enter the Security password from Required Installation Information.
- Note** The Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between nodes, and you must ensure this password is identical on all nodes in the cluster.
- The **SMTP Host Configuration** window appears.
- Step 4** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name. If you do not want to configure the SMTP server, choose **No**, which redirects to Smart Call Home page. To go to previous page, choose **Back** and to see the information about the SMTP configuration, choose **Help**.
- Note** You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.
- Step 5** Choose **OK**. The **Smart Call Home Enable** window appears.
- Step 6** On the Smart Call Home Enable Page, perform one of the following.
- a) Select **Enable Smart Call Home on System Start** to enable the Call Home, and then click **OK**. The Smart Call Home Configuration window appears.
 1. Select the method for sending data to the Cisco Technical Assistance Center.
 - Secure Web (HTTPS)
 - Secure Web (HTTPS) through Proxy

Enter the Hostname/IP Address and port number for Proxy

- Hostname/IP Address—Enter the IP address or the hostname of the proxy server to send the Call Home messages through an indirect network connection.
- Port—Enter the port number on which the proxy server is enabled.

- Email

Note You must have configured the SMTP for Email to be sent successfully.

2. To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.
3. Enter the email address of the customer in the Customer Contact Details field.
4. Click **Continue** to proceed, or select **Back** to return to the previous menu. If you click **Continue**, a message appears as Cisco Call Home includes reporting capabilities that allow Cisco to receive diagnostic and system information from your Unified Communications Manager cluster. Cisco may use this information for proactive debugging, product development or marketing purposes. To learn more about this feature, please visit: http://www.cisco.com/en/US/products/ps7334/serv_home.html.

Note If you select **Secure Web (HTTPS) through Proxy** and click **Continue**, Smart Call Home Proxy Configuration Page appears.

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

- b) Select **Enable Anonymous Call Home on System Start** to enable the Anonymous Call Home, and then click **OK**. The Anonymous Call Home Configuration window appears.

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

- Secure Web (HTTPS)
- Secure Web (HTTPS) through Proxy

Enter the Hostname/IP Address and port number for Proxy

- Hostname/IP Address—Enter the IP address or the hostname of the proxy server to send the Call Home messages through an indirect network connection.
- Port—Enter the port number on which the proxy server is enabled.

- Email

Note You must have configured the SMTP for Email to be sent successfully.

2. To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.
3. Click **Continue** to proceed, or select **Back** to return to the previous menu. If you click **Continue**, a message appears as To help improve the Cisco Unified Communications Manager experience, click Confirm to allow Cisco Systems to securely receive usage statistics from the server. This information will be used by

Cisco to help understand how customers are using our product and ultimately drive product direction. If you prefer not to participate, you may choose to opt-out.

Note If you select **Secure Web (HTTPS) through Proxy** and click **Continue**, Anonymous Call Home Proxy Configuration Page appears.

4. Click **Confirm** to proceed with normal installation or select **Back** to return to the Smart Call Home Enable Page.
- c) Select **Remind me Later to configure Smart Call Home** to configure the Smart Call Home service after installation, using Cisco Unified Serviceability pages.

A reminder message appears in Cisco Unified CM Administration.

Smart Call Home is not configured. To configure Smart Call Home or disable the reminder, please go to Cisco Unified Serviceability > Call Home.

- d) Select **Disable All Call Home on System Start** to disable the Smart Call Home service. However, you can activate the Smart Call Home service after installation using Cisco Unified Serviceability pages.

Note You can reconfigure the service in Cisco Unified Serviceability page after installation. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Step 7 Choose **OK**. The Application User Configuration window appears.

Step 8 Enter the Application User name and password from and confirm the password by entering it again.

Step 9 Choose **OK**. The Platform Configuration Confirmation window appears.

Step 10 To continue with the installation, choose **OK**; or to modify the platform configuration, choose **Back**.

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

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

Set Up Subscriber Node

Use the following procedure to configure a subscriber node in the cluster.

Before you begin

For both Cisco Unified Communications Manager and IM and Presence Service subscriber nodes, you must add the node in the Server Configuration window (System > Server) on the Cisco Unified Communications Manager publisher node before you complete this procedure.

For information on how to add a node to a cluster, see the *Administration Guide for Cisco Unified Communications Manager*.

Procedure

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

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

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

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

- To pause the installation after the system successfully verifies network connectivity, choose **Yes**.
- To continue the installation with a pause, choose **No**.

The First Node Access Configuration window displays.

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

The system checks for network connectivity.

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

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

The **SMTP Host Configuration** window displays.

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

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

The Platform Configuration Confirmation window displays.

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

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