Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 9.0(1)

First Published: July 18, 2012

Last Modified: July 18, 2012

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

Text Part Number: OL-27194-01

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 NONINFRINGEMENT 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface vii

Purpose vii

Audience vii

Organization vii

Related Documentation viii

Conventions viii

Obtain Documentation and Submit Service Requests x

Cisco Product Security Overview x

CHAPTER 1

New in this release 1

Software version restrictions 1

Upgrade order 2

Standard upgrade order 2

Refresh upgrade order 3

PART I

Software Upgrades for Unified CM 5

CHAPTER 2

Software Upgrades 7

Pre-Upgrade Tasks 7

Upgrade Considerations 9

Software Upgrade Process Overview 10

Upgrade Configuration Changes 11

Administration Changes 11

Upgrade Tasks 12

User Provisioning 13

Upgrade a Cluster 13

Supported Upgrades 14

Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager 15
Obtain Upgrade File 15
Software Upgrade Procedures 15
Local Source Software Upgrade 15
Upgrade From Local Source 15
Remote Source Upgrade 16
SFTP Server Support 16
Remote Source Software Upgrade 17
Bridge Upgrade 18
Post-Upgrade Tasks 20
Reduced Permissions for Access Control Groups 21
Switch to Previous Version 21
Switch Cluster to Previous Version 21
Switch Node to Previous Version 22
Reset Database Replication 22
COP Files, Dial Plans, and Locales 23
COP File Installation 23
Dial Plan Installation 23
Locale Installation 23
Locale Installation Considerations 24
Locale Files 24
Error Messages 25
Supported Products 26
Manage TFTP Server Files 26
Set Up a Custom Log-On Message 27

PART II **Software Upgrades for IM and Presence Service** 29

CHAPTER 3 **Before you begin** 31
Read this first 31
System availability after upgrade 32
Support for intercluster peers 32
Multinode clusters 32

Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager 32
Types of upgrades 32
Standard upgrades 33
Refresh upgrades 33
Refresh upgrade overview 34
Special considerations for refresh upgrade 35
MCS-7825-H3 or MCS-7828-H3 server upgrade 35
COP File Installation 35
Refresh upgrade stages 35
Upgrade time requirements 36
Throttling affects time required to upgrade 36
License requirements 36
Bridged upgrade 36
Upgrade paths, requirements, and restrictions 37
Software version restrictions 37
Version Switching Rules 38
Manual switching rules 38
Version Switching During Upgrade Rules 38
Upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5(4) 38
User Profile Data Migration 39
Intercluster upgrades 41
Perform pre-upgrade tasks 41

CHAPTER 4 **Upgrade procedures** 43
Multinode software upgrade procedures 43
Perform a Standard Upgrade 44
Perform a Refresh Upgrade 46
Software procedures 47
Upgrade from local source 48
Upgrade from remote source 50
Upgrade to IM and Presence on virtual server 51
Switch software version 52
Revert to previous software version 53
Switch version back to Cisco Unified Presence 8.6(3) or earlier 54

CHAPTER 5 Post-upgrade tasks 57

High Availability 57

Verify IM and Presence Service Data Migration 57

CHAPTER 6 Troubleshooting 59

IM and Presence user phone presence problems 59

Presence User Experiences Issues Obtaining Availability 59

Real-Time Monitoring Tool alert for Cisco SIP proxy service 60

Cannot find upgrade file on remote server 60

Upgrade file checksum values do not match 60

Database replication did not complete 60

Cisco UP Presence Engine database does not restart 60

Version Errors 61

Failed refresh upgrade 61

Cancelled or failed upgrade 61

Upgrade From Pre Release 8.6(4) Fails 61

Directory Was Located and Searched but No Valid Options or Upgrades Were Available 62

CHAPTER 7 Reference 63

Effects of I/O throttling 63

Overview 63

Disable throttling 63

Server models 63

Write-cache 64

Locale specific upgrades 66

About Locales 66

Locale installation 66

Preface

- Purpose, page vii
- Audience, page vii
- Organization, page vii
- Related Documentation, page viii
- Conventions, page viii
- Obtain Documentation and Submit Service Requests, page x
- Cisco Product Security Overview, page x

Purpose

This document provides information about upgrading software.

Audience

This Upgrade Guide is intended for administrators who are responsible for upgrading the following software:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Business Edition 5000
- IM and Presence Service on Cisco Unified Communications Manager

Organization

The following table shows how this guide is organized:

Chapter	Description
Part 1	“Software upgrades for Cisco Unified Communications Manager” Provides instructions to upgrade Cisco Unified Communications Manager to Release 9.x.
Part 2	“Software upgrades for IM and Presence Service” Provides instructions to upgrade the IM and Presence Service to Release 9.x.

Related Documentation

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

- *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 related Cisco IP telephony applications and products, refer to the Cisco Unified Communications Manager Documentation Guide for your release at

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

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.

Convention	Description
{ 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.
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 D key.
< >	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 Documentation and Submit Service Requests

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

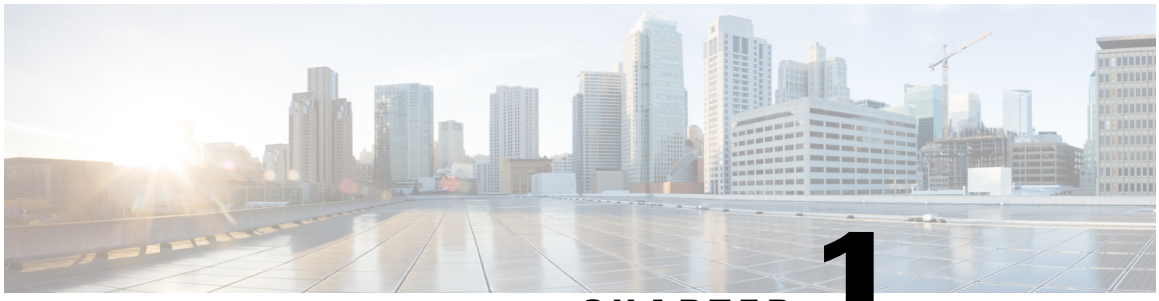
Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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.

Further information regarding U.S. export regulations may be found at

http://www.access.gpo.gov/bis/ear/ear_data.html



CHAPTER 1

New in this release

The following chapter describes important upgrade information for Cisco Unified Communications Manager Release 9.0(1) and the IM and Presence Service Release 9.0(1).

- Software version restrictions, page 1
- Upgrade order, page 2

Software version restrictions

Unified Communications Manager and IM and Presence Service software versions must have the same major and minor release number. Major and minor release numbers are defined as follows:

`9.x.y`

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

For example, IM and Presence Release 9.0.2.10000-4 is compatible with Unified Communications Manager Release 9.0.12.30000-2, but it is not compatible with Unified Communications Manager Release 9.1.1.10000-3. Similarly, Unified Communications Manager Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-9.

The software version of subsequent IM and Presence nodes that you upgrade must match all five version numbers of the first IM and Presence node that you upgraded.

Note You cannot upgrade IM and Presence unless the upgraded release of Unified Communications Manager is already installed on the active or inactive partition. You must upgrade Unified Communications Manager before you can upgrade IM and Presence to the matching version.

Caution If you use Platform Administrative Web Services (PAWS) Management to upgrade IM and Presence, do not attempt to upgrade and reboot to the current IM and Presence release if the active partition on Unified CM is running an incompatible software version. If you do, the upgrade will fail, as expected, but the failure will not be reported until near the end of the upgrade process. You will also experience system downtime when the system reboots.

The delayed upgrade failure notification applies only to upgrades that are performed with PAWS Management. If you perform the upgrade through Cisco Unified IM and Presence Operating System Administration or through the CLI, the upgrade failure notification is displayed at the beginning of the upgrade.

Upgrade order

The order in which you upgrade Cisco Unified Communications Manager (Unified CM) and IM and Presence is very important.

Note Do not start to upgrade the IM and Presence publisher node until the upgrade of the Unified CM publisher node has reached a specified point. See the section *Upgrade a Cluster* for more information about determining the specified point in the upgrade.

Do not start to upgrade an IM and Presence subscriber node until the upgrade of the IM and Presence publisher node is complete.

Related Topics

Upgrade a Cluster, on page 13

Standard upgrade order

The following upgrade paths are standard upgrades:

- Unified CM Release 8.6.x to Unified CM Release 9.0(1)
- Cisco Unified Presence Release 8.6(4) to IM and Presence Service Release 9.0(1)

For standard upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified CM publisher node.
2. Upgrade the IM and Presence publisher node and the Unified CM subscriber nodes.
3. Upgrade the IM and Presence subscriber nodes.
4. Switch versions on the Unified CM publisher node.
5. Switch versions on the IM and Presence publisher node and Unified CM subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Note For Unified CM upgrades, follow the instructions in Part I of this document. For IM and Presence upgrades, follow the instructions in Part II of this document.

Refresh upgrade order

The following upgrade paths are refresh upgrades:

- Unified CM Release 8.5 and earlier to Unified CM Release 9.0(1)
- Cisco Unified Presence Release 8.6(3) and earlier to IM and Presence Service Release 9.0(1)

For refresh upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified CM publisher node
2. Switch versions on the Unified CM publisher node.
3. Upgrade the IM and Presence publisher node and the Unified CM subscriber nodes.
4. Switch versions on the IM and Presence publisher node and Unified CM subscriber nodes.
5. Upgrade the IM and Presence subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Note For Unified CM upgrades, follow the instructions in Part I of this document. For IM and Presence upgrades, follow the instructions in Part II of this document.

Refresh upgrades for Unified CM are described in the topic “Software upgrade process overview.”

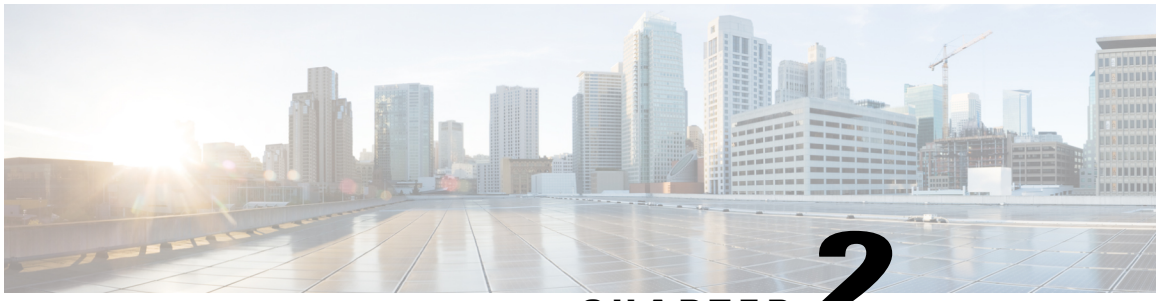
Related Topics

Software Upgrade Process Overview, on page 10

PART I

Software Upgrades for Unified CM

- Software Upgrades, page 7



CHAPTER 2

Software Upgrades

- Pre-Upgrade Tasks, page 7
- Upgrade Considerations, page 9
- Software Upgrade Procedures, page 15
- Post-Upgrade Tasks, page 20
- Switch to Previous Version, page 21
- COP Files, Dial Plans, and Locales, page 23
- Manage TFTP Server Files, page 26
- Set Up a Custom Log-On Message, page 27

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

- Read the release notes for the new release and be sure that you understand the new features and how the upgrade interacts with the other products that are associated with your system, such as JTAPI, CUMA (Cisco Unified Manager Assistant), RTMT, IPCC, firewalls, and so on.

  For Cisco Unified Communications Manager, the release notes are located at

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

- Ensure that you have the necessary license files for the new release.

  For more information on obtaining and installing licenses, see the License File Upload chapter in the *Cisco Unified Communications Manager Administration Guide*.

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

Warning You must apply all pre-9.0 licenses to Cisco Unified Communications Manager before you upgrade to Release 9.0 or later software. After you upgrade to Release 9.0 or later software, you cannot apply these licenses to Cisco Unified Communications Manager and you cannot apply them using the Enterprise License Manager. Ensure that you install all unused licenses or Product Authorization Keys (PAKs) before you upgrade the system. The Cisco Unified Communications Manager displays a warning to prompt you to install any unused licenses before proceeding.

- Before you begin the upgrade, back up your system. This is particularly important if you are upgrading software on HP7825H3 or HP7828H3 hardware as there is no option to revert to the previous version.
- If you are upgrading software on HP7825H3 or HP7828H3 hardware, ensure that you have a 16GB USB device available to migrate your data to the new system. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.
- Disable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability** > **Tools** > **Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Note Be aware that, when you deactivate the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

- Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.
- Before you upgrade to a later release, refer to the documentation for your currently installed COP files to identify any special considerations related to upgrading Cisco Unified Communications Manager.
- If you plan to use IPv6 with Cisco Unified Communications Manager Release 8.0(2) or later, you can provision your DNS server for IPv6 prior to upgrading to Release 8.0(2) or later. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you perform the upgrade.

Caution Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.0(2) or later causes the upgrade to fail.

- Before you upgrade a cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (publisher node) and subsequent nodes (subscriber nodes). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.
- Use the **utils dbreplication setrepltimeout** CLI command to increase the database replication timeout value when upgrading large clusters so that more subscriber nodes have sufficient time to request replication. When the timer expires, the first subscriber node, plus all other subscriber nodes that requested replication within that time period, begin a batch data replication with the publisher node. The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the subscriber nodes have successfully set up replication. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
- Before you perform the Cisco Unified Communications Manager upgrade, ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.
- Review the following related topic after you complete the pre-upgrade tasks.

Note We recommend that you install and assign the Cisco Unified CM "vcs-interop" SIP Normalization script to make secure calls between CTS endpoints and endpoints and devices registered to VCS.
For more information about the conditions required for secure calls, see this document:

http://www.cisco.com/en/US/docs/telepresence/cts_admin/1_8/release/notes/cts_1_8_release_notes.html#wp138743
For more information about the Cisco Unified CM script, see this document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/8_6_2/cucm-rel_notes-862.html#wp1961382
For more information about configuring Cisco Unified CM and Cisco VCS to interoperate via a SIP trunk, see this document:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Cisco_Unified_Communications_Manager_Deployment_Guide_CUCM_6-1_7_8_and_X7-0.pdf

Related Topics

Upgrade Considerations, on page 9

Upgrade Considerations

This section contains topics which should be reviewed prior to performing an upgrade.

Caution There is a known issue with upgrades from Unified CM 6.x or 7.x. Upgrades from these releases may fail with the upgrade installdb log indicating a communication or connection issue in BulkMigration. This issue is noted in CSCts34871. The workaround is to reboot the system and perform the upgrade again. See CSCts34871 in Bug Toolkit on Cisco.com for further details.

Software Upgrade Process Overview

You cannot install upgrade software on your node while the system continues to operate.

Caution If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

When you install upgrade software, there will be a temporary node outage while the Cisco Unified Communications Manager software is installed. Once you kick off the upgrade using either the command line or graphical user interface the data will be exported, and the system will be automatically rebooted at which point the node outage will begin. The duration of this outage will depend on your configuration and amount of data. During the upgrade, progress can be monitored via the console until such time that command line interface and graphical user interface access has been restored. Once restored, you can use the command line interface or graphical user interface to continue to monitor upgrade progress.

Note If an administrator or a phone user makes changes during the upgrade process (export of data), that data could be lost after upgrade.

When you initiate the upgrade, you can indicate to activate the partition with the new upgrade software or return to using the partition with the previous version of the software at upgrade completion. With the exception of HP 7825H3 and HP7828H3 hardware upgrades, the previous software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

When you upgrade a cluster, start by upgrading the publisher node. You can begin upgrading subsequent nodes in parallel after the publisher node reaches a specified point in the upgrade. There will be a temporary node outage until all subscriber nodes get upgraded to the new software version. See the section *Upgrade a cluster* for more information about determining when to begin upgrading subsequent nodes.

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

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since you upgraded the software will get lost.

Note You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

If the upgrade of a subsequent node fails after you upgrade the publisher node and switch it to the new version or fail to upgrade one of the subsequent nodes in your cluster during the upgrade cycle, you can do one of the following:

- Correct the errors that caused the upgrade failure on the subsequent node. You may want to check the network connectivity of the nodes in your cluster, reboot the subsequent node, ensure the node memory and CPU usage on the subsequent node is not too high. Upgrade the subsequent node again.
- Make sure that the active partition of the publisher node runs the newest version of software installed on the node. Perform a fresh installation on the subsequent node using the same software version as that running on the active partition of the publisher node. If you are reinstalling the subsequent node, you should delete the node from Cisco Unified Communications Manager Administration and add the node again as described in the *Cisco Unified Communications Manager Administration Guide*.

You can upgrade from a DVD (local source) or from a network location (remote source) that the node can access.

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

Note Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Related Topics

Upgrade a Cluster, on page 13

Upgrade Configuration Changes

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration Changes

The administrator must not make any configuration changes to Cisco Unified Communications Manager during an upgrade. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option windows.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

If you are upgrading your system, you must complete the upgrade tasks in this section before you perform any configuration tasks.

Caution If you fail to follow these recommendations, unexpected behavior may occur; for example, ports may not initialize as expected.

Upgrade Tasks

To successfully complete the upgrade, perform the upgrade tasks in the following order before you begin making configuration changes.

Note Cisco strongly recommends that you do not perform configuration tasks until the upgrade completes on all nodes in the cluster, until you have switched the nodes over to the upgraded partition, and until you have verified that database replication is functioning.

For more information, see the refresh upgrade procedure in the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 If you are performing a refresh upgrade from Cisco Unified Communications Manager Release 7.x, see the *Cisco Unified Communications Manager Security Guide* for more information about the upgrade procedure.

Step 2 Stop all configuration tasks; that is, do not perform configuration tasks in the various Cisco Unified Communications Manager-related GUIs or the CLI (with the exception of performing the upgrade in the Cisco Unified Communications Operating System GUI).

Step 3 Upgrade the first node in the cluster (the publisher node).

Note If performing an L2 upgrade, choose no for automatic reboot. The switch version will occur in step 4.

Note If performing an refresh upgrade, choose to run new version at the completion of the upgrade. Step 4 is not required.

Step 4 Upgrade the subsequent nodes in the cluster (the subscriber nodes).

Note If performing an L2 upgrade, choose no for automatic reboot. The switch version will occur in step 5.

Note If performing an refresh upgrade, choose to run new version at the completion of the upgrade. Step 5 is not required.

Step 5 Switch over the first node to the upgraded partition.

Step 6 Switch over subsequent nodes to the upgraded partition.

Note You can switch the subsequent nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 7 Ensure that database replication is functioning between the first node and the subsequent nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified CM Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:

- 0 - Initializing.
- 1 - Replication setup script fired from this node.
- 2 - Good replication.
- 3 - Bad replication.
- 4 - Replication setup did not succeed.

Before you proceed, ensure that you have a good database replication status. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

User Provisioning

For upgrades from Cisco Unified Communications Manager Release 8.x, changes that are made to the following user-facing features get preserved after the upgrade completes:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication
- Recording enabling
- Single Number Reach enabling

Upgrade a Cluster

When you upgrade a cluster, begin upgrading the publisher node first. You can begin upgrading subsequent nodes after the publisher node has finished upgrading. There will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

During the upgrade of the publisher node, you can view the installation log, install_log_<date+time>.log, by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or the command line interface (CLI). You can also use the CLI to search for the relevant information in the install log by following this procedure:

Procedure

Step 1 List the install logs; for example:

```
file list install install_* date
install_log_2008-10-01.09.41.57.log    install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

Step 2 Search the most recent install log for the string PRODUCT_VERSION; for example:

```
admin:file search install install_log_2013-01-07.09.39.11.log
PRODUCT_VERSION

Searching path: /var/log/install/install_log_2013-01-07.09.39.11.log
Searching file: /var/log/install/install_log_2013-01-07.09.39.11.log
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION is
9.1.1.10000-11|<LVL::Info>
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION_DISPLAY is
9.1.1.10000-11|<LVL::Info>
Search completed
```

What to Do Next

After the publisher node has been upgraded, you can start to upgrade the subsequent nodes. When you are ready to activate the new version, you must activate the new software on the publisher node before activating it on all other nodes.

Caution If you attempt to upgrade the subsequent nodes in parallel with the publisher node, do not choose the Reboot to upgraded partition on either publisher node or subsequent nodes while configuring the upgrade options. If selected, the publisher node may complete its upgrade and reboot while the subsequent nodes are upgrading, which causes the upgrade of the subsequent nodes to fail.

Supported Upgrades

For information about supported upgrades, see the Release Notes for your product release and the Cisco Unified Communications Manager Compatibility Matrix at the following URL:

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

Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager

There is no upgrade path in VMware to upgrade from Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager. A fresh installation is needed. After you perform the fresh installation, IM and Presence Service re-synchronizes data with the new Cisco Unified Communications Manager. The Syncagent uses the primary key (pkid) as a comparison field for the synchronization. When the Cisco Unified Communications Manager is re-installed, all the pkid on Cisco Unified Communications Manager are changed. As such, any existing data on IM and Presence Service is cleaned up and the Syncagent deletes the old data. Be sure to backup your data before performing this procedure.

Obtain Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Software Upgrade Procedures

This section provides procedures for upgrading from either a local or a remote source.

Local Source Software Upgrade

Upgrade From Local Source

To upgrade the software from local DVD, follow this procedure:

Procedure

Step 1 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Step 2 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Note Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks.

Step 3 Insert the new DVD into the disc drive on the local server that is to be upgraded.

Step 4 Log in to Cisco Unified Communications Operating System Administration.

Step 5 Navigate to **Software Upgrades** > **Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 6 From the **Source** list, choose **DVD**.

Step 7 Enter a slash (/) in the Directory field.

Step 8 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 9 To continue the upgrade process, click **Next**.

Step 10 Choose the upgrade version that you want to install and click **Next**.

Step 11 In the next window, monitor the progress of the download.

Step 12 If you want to run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software.

Step 13 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps:

a) Choose **Do not switch to new version after upgrade**.

b) Click **Next**.
The Upgrade Status window displays the Upgrade log.

c) When the installation completes, click **Finish**.

d) To restart the system and activate the upgrade, choose **Settings** > **Version**; then, click **Switch Version**.
The system restarts running the upgraded software.

Remote Source Upgrade

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

SFTP Server Support

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 versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

`http://www.cisco.com/pcgi-bin/ctdp/Search.pl`

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

`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 (refer to `http://sshwindows.sourceforge.net/`)
- Cygwin (refer to `http://www.cygwin.com/`)
- Titan (refer to `http://www.titanftp.com/`)

Cisco does not support using the SFTP product free FTDP. This is because of the 1GB file size limit on this SFTP product.

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

Remote Source Software Upgrade

To upgrade the software from a network location or remote server, use the following procedure.

Note Do not use the browser controls, such as Refresh/Reload, while you are accessing Cisco Unified Communications Operating System Administration. Instead, use the navigation controls that are provided by the interface.

Procedure

Step 1 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Step 2 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

Step 3 Log in to Cisco Unified Communications Operating System Administration.

Step 4 Navigate to **Software Upgrades** > **Install/Upgrade**.
The Software Installation/Upgrade window displays.

Step 5 From the **Source** list, choose **Remote Filesystem**.

Step 6 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.
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

a) Begin the path with a forward slash (/) and use forward slashes throughout the path.

b) 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:).

Step 7 In the **Server** field, enter the server name or IP address.

Step 8 In the **User Name** field, enter your user name on the remote server.

Step 9 In the **User Password** field, enter your password on the remote server.

Step 10 Select the transfer protocol from the **Transfer Protocol** field.

Step 11 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 12 To continue the upgrade process, click **Next**.

Step 13 Choose the upgrade version that you want to install and click **Next**.

Step 14 In the next window, monitor the progress of the download.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again:

Note Warning: Another session is installing software, click Assume Control to take over the installation.

Note If you are sure you want to take over the session, click **Assume Control**.

Note If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 15 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.

Step 16 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, complete the following steps:

a) Choose **Do not switch to new version after upgrade**.

b) Click **Next**.
The Upgrade Status window displays the Upgrade log.

c) When the installation completes, click **Finish**.

d) To restart the system and activate the upgrade, choose **Settings** > **Version**; then, click **Switch Version**.
The system restarts and is running the upgraded software.

Bridge Upgrade

The bridge upgrade provides a migration path for customers who want to migrate from discontinued Cisco Unified Communications Manager server to a node that supports the newest release of Cisco Unified Communications Manager.

Servers that are no longer supported, but are permitted to function as bridge upgrade nodes, can upgrade and boot but will not allow Cisco Unified Communications Manager to function.

When you attempt to upgrade your Cisco Unified Communications Manager version on a discontinued server model, Cisco Unified Communications Manager inserts a message into the upgrade log. The upgrade log is displayed on the web browser when the upgrade is initiated through the Cisco Unified Communications Operating System Administration window, or you can view it through CLI if you used CLI to perform the upgrade. This message notes that you can only use the new version to obtain a DRS backup. The warning message in the log is followed by a delay that allows you to cancel the upgrade if you do not want to do a bridge upgrade.

When the system boots the new Cisco Unified Communications Manager version, a warning appears on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality."). Because of the restricted visibility of the console, the warning displays during both CLI and GUI sessions.

Note During a bridge upgrade, if the only upgrade is to the publisher (rather than to all nodes in the cluster) all subscribers must be offline.

Use the following procedure to perform a bridge upgrade:

Procedure

Step 1 Perform an upgrade to the new Cisco Unified Communications Manager version on your discontinued first node (publisher node). Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do. Observe the warning on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality.").

Step 2 Perform an upgrade to the new Cisco Unified Communications Manager version on your subsequent node (subscriber nodes). Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do.

Step 3 Verify database synchronization between all nodes. You can use the CLI commands utils dbreplication runtime state and utils dbreplication status. For more information, refer to the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 4 Using the new Cisco Unified Communications Manager version on your discontinued first node server, perform a DRS backup. The DRS backups are encrypted using the cluster security password provided at install time. You must remember this security password as the "old" password, because you may be prompted to enter this "old" password at the time of restore. Refer to the Disaster Recovery System Administration Guide.

Step 5 Disconnect your discontinued server from the network.

Step 6 Install the new Cisco Unified Communications Manager version on your new supported first node. You must obtain and install a new license on this node. Refer to the guide Installing Cisco Unified Communications Manager. You will be prompted to enter a "new" security password, a password that is different from the "old" password you noted in the previous step. The guide Installing Cisco Unified Communications Manager describes the requirements of a "new" security password that Cisco Unified Communications Manager will accept. You must remember this "new" security password.

Step 7 Using the new Cisco Unified Communications Manager version on your new supported first node, perform the Disaster Recovery System Administration Guide procedure "Restoring the First Node only (Rebuilding the Publisher Alone)". First, select only select the first node for restore. You can only select the subsequent nodes for restore after the completion of first node restore. Use the discontinued server's backup file that you created previously. You will be prompted for the "old" security password that you noted previously. For further details, refer to the *Disaster Recovery System Administration Guide*.

Step 8 On your new supported first node, reactivate all services that used to be active on your discontinued first node server before the bridge upgrade. Refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Step 9 Verify database synchronization between all nodes. You can use the CLI commands **utils dbreplication runtime state** and **utils dbreplication status**. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Post-Upgrade Tasks

After the upgrade, perform the following tasks:

- If you changed the database replication timeout value for the upgrade using the **utils dbreplication setrepltimeout** CLI command, restore the timeout to the default value of 300 (5 minutes). For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
- Enable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability** > **Tools** > **Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Note If you do not enable the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line
- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
  - Do Not Disturb
  - Privacy
  - Presence
  - CTI call control
  - Busy Lamp Field
- If necessary, reinstall the Real Time Monitoring Tool.

Note After you perform a switch version when you upgrade Unified CM, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Reduced Permissions for Access Control Groups

Problem When you add a new access control group to existing users, the level of privileges for some pre-existing access control groups is unexpectedly reduced.

Solution Users can belong to multiple access control groups. When you add a new access control group to existing users, the current level of privileges for some pre-existing access control groups may be reduced if the new access control group has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Switch to Previous Version

If you need to revert to the software version that was running before the upgrade, you can do so by using the Switch Version option to switch the system to the software version on the inactive partition.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, a 128GB external USB device is required.

Switch Cluster to Previous Version

If you downgrade a cluster to a nonsecure previous release of Cisco Unified Communications Manager (prior to release 8.0), you must prepare the cluster for rollback before you switch versions. If you do not prepare the cluster for rollback before you revert to a previous release, you have to manually delete the ITL file on each Cisco Unified IP Phone in the system. For more information, see the *Cisco Unified Communications Manager Security Guide*.

To switch a cluster back to a previous version, complete these high-level tasks:

Procedure

Step 1 Switch back the publisher node.

Step 2 Switch back all backup subscriber nodes.

Step 3 Switch back all primary subscriber nodes.

Step 4 If you are reverting to an older product release, reset database replication within the cluster.

Related Topics

Switch Node to Previous Version, on page 22
Reset Database Replication, on page 22

Switch Node to Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
https://node-name/**cmplatform**

where node-name specifies the host name or IP address of the Cisco Unified Communications Manager node.

Step 2 Enter your Administrator user name and password.

Step 3 Choose **Settings** > **Version**.
The Version Settings window displays.

Step 4 Click the **Switch Versions** button.
After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 To verify that the version switch was successful, follow these steps:

a) Log in to Cisco Unified Communications Operating System Administration again.
b) Choose **Settings** > **Version**.
The Version Settings window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.
e) For the publisher node, log in to Cisco Unified CM Administration.
f) Verify that you can log in and that your configuration data exists.

Reset Database Replication

If you switch back the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command **utils dbreplication reset all** on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message that reminds you about the requirement to reset database replication if you are reverting to an older product release.

COP Files, Dial Plans, and Locales

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

COP File Installation

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

- Install the appropriate COP file on every node in a cluster. Perform this task before you install new software on each node in the cluster and set up the database.
- After you install a COP file, you must restart the node.
- Restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database.

Dial Plan Installation

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

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

Locale Installation

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

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

Tip Since the primary language spoken in Belgium is Dutch, you can download the Dutch (Netherlands) locale file, for example, cm-locale-nl_NL- 8.5.1.2100-1.cop.sgn (Cisco Unified Communications Locale Installer 8.5.1.21000-1 Dutch (Netherlands)). Secondary languages commonly spoken in Belgium are French and German.

User Locales

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

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

If your system requires user locales only, install them after you have installed the CUCM locale.

Network Locales

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

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

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

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

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

Locale Installation Considerations

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

You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

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

Locale Files

When you install locales on a node, install the following files:

- User Locale files - These files contain language information for a specific language and country and use the following convention:

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

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

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

Error Messages

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

Table 1: Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable	This error occurs because a Cisco Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified Communications Manager database. If this application is not found, it either was not installed with Cisco Unified Communications Manager (very unlikely), has been deleted (more likely), or the node does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.

Message	Description
[LOCALE] Could not create /usr/local/cm/application_locale /cmservices/ipma/com/cisco/ipma /client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/ application_locale/cmservices/ipma/com/cisco/ ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/ application_locale/cmservices/ipma/ LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMaster Version.txt in order to update Unified CM Assistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Supported Products

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager, which is available at this URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51`

Manage TFTP Server Files

You can upload files for use by the phones to the TFTP server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the tftp directory by default. You can also upload files to a subdirectory of the tftp directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all nodes, nor to both Cisco TFTP servers in a cluster.

To upload and delete TFTP server files, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **TFTP** > **File Management**.
The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

Step 2 To upload a file, follow this procedure:

a) Click **Upload File**.
The Upload File dialog box opens.

b) To upload a file, click **Browse** and then choose the file that you want to upload.

c) To upload the file to a subdirectory of the tftp directory, enter the subdirectory in the **Directory** field.

d) To start the upload, click **Upload File**.
The Status area indicates when the file uploads successfully.

e) After the file uploads, restart the Cisco TFTP service.

Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.

For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide*.

Step 3 To delete files, follow this procedure:

a) Check the check boxes next to the files that you want to delete.
You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

b) Click **Delete Selected**.

Note If you want to modify a file that is already in the tftp directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Set Up a Custom Log-On Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to Software **Upgrades** > **Customized Logon Message**.
The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10kB.

The system displays the customized log-on message.

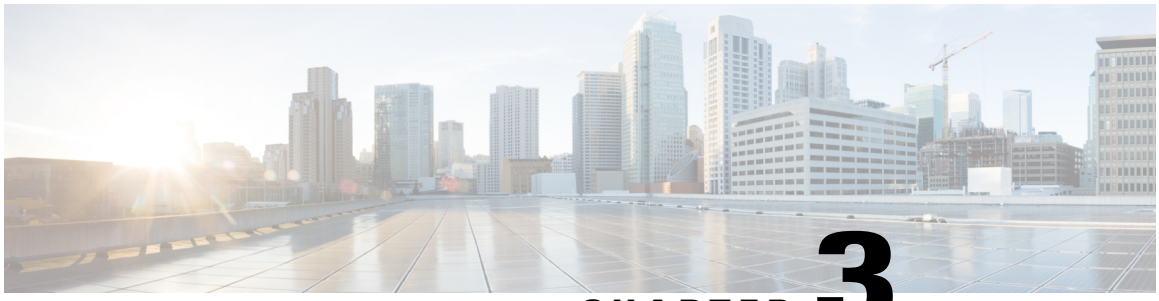
Step 4 To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

PART II

Software Upgrades for IM and Presence Service

- Before you begin, page 31
- Upgrade procedures, page 43
- Post-upgrade tasks, page 57
- Troubleshooting, page 59
- Reference, page 63



CHAPTER 3

Before you begin

This chapter discusses how you should prepare to upgrade to a new release of the IM and Presence Service.

- Read this first, page 31
- Types of upgrades, page 32
- Refresh upgrade overview, page 34
- Upgrade time requirements, page 36
- License requirements, page 36
- Bridged upgrade, page 36
- Upgrade paths, requirements, and restrictions, page 37
- User Profile Data Migration, page 39
- Intercluster upgrades, page 41
- Perform pre-upgrade tasks, page 41

Read this first

Read the following important notes before you begin an upgrade.

Warning Do not make any changes to IM and Presence configuration during an upgrade. If data is written to the database during the upgrade, the upgrade may fail.

Warning Do not delete any users during the time that you initiate a standard upgrade and switch to the new software version. Deleting users on Cisco Unified Communications Manager (Unified CM) during this time period causes the migration of the UC Profile data from Cisco Unified Presence to Unified CM to fail.

Also, during the time that you initiate a standard upgrade and switch to the new software version, do not perform an LDAP sync that may delete users because this action will cause the migration of the UC Profile data to fail.

- All refresh upgrades must be performed during a maintenance window because the system will not be available during the upgrade.
- If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence server before you attempt another upgrade.

System availability after upgrade

For standard upgrades, when you activate the upgraded software, the system restarts and is out of service for up to 30 minutes on the publisher node, depending on the size of the database. The length of the outage on subscriber nodes depends on how long database replication takes to complete.

If you need to revert to an earlier software version, you must restart the system which results in a similar service outage period.

Support for intercluster peers

This release of IM and Presence supports intercluster peers to clusters running Cisco Unified Presence Release 8.6 and IM and Presence Release 9.x. Intercluster peers to clusters running Release 8.0(x) or Release 8.5(x) are not supported.

Multinode clusters

If you have an IM and Presence cluster comprising multiple nodes, you must upgrade all nodes in the cluster. If you have a multinode cluster, you must upgrade the publisher node prior to upgrading the subscriber nodes. Also, you cannot perform a fresh installation on the publisher node and then perform an upgrade on subscriber nodes.

Presence Data Loss After Upgrade Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager

There is no upgrade path in VMware to upgrade from Cisco Unified Business Edition 5000 to Cisco Unified Communications Manager. A fresh installation is needed. After you perform the fresh installation, IM and Presence Service re-synchronizes data with the new Cisco Unified Communications Manager. The Syncagent uses the primary key (pkid) as a comparison field for the synchronization. When the Cisco Unified Communications Manager is re-installed, all the pkid on Cisco Unified Communications Manager are changed. As such, any existing data on IM and Presence Service is cleaned up and the Syncagent deletes the old data. Be sure to backup your data before performing this procedure.

Types of upgrades

There are two types of upgrades:

- standard upgrades
- standard upgrades—upgrades which do not upgrade the operating system and do not require multiple reboots during installation. You can install upgrade software on your server while the system continues to operate.
- refresh upgrades

- refresh upgrades—refresh upgrades are required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the operating system (OS) changes between the version you are upgrading from and the version that you are upgrading to. Refresh upgrades require multiple reboots during installation to upgrade the underlying operating system.

The server automatically determines whether you need to perform a standard upgrade or a refresh upgrade.

Standard upgrades

For standard upgrades, you install the upgrade software as an inactive version. The system continues to function normally while you are installing the software. When the upgrade is complete, you can choose to automatically reboot the system to the upgraded software or you can manually switch to the new software at a later time. When you reboot to the new software, the old software version remains on the system. This allows you to switch back to the old version in the unlikely event of issues with the new software. During an upgrade your configuration information migrates automatically to the upgraded version.

Note You can only make changes to the database on the active software. The database for the inactive software is not updated. If you make changes to the database after an upgrade, you must repeat those changes after switching to the new software.

Refresh upgrades

Note You must perform all refresh upgrades during a maintenance window because the system will not be available during the upgrade.

For refresh upgrades, the upgrade wizard allows you to choose whether or not to automatically run the new upgrade software when the upgrade completes. If you select not to run the new software, the system will reboot to the old software version when the upgrade is complete and you can manually switch to the new software at a later time.

If for any reason you decide to revert to the prior software version, you can switch versions to the older version of the software. This switch version requires a reboot. Be aware that any configuration changes that you made after upgrading the software will be lost.

If you downgrade to Cisco Unified Presence Release 8.6(3) or earlier, you must install a COP file after you switch to the older software version.

Note If you deploy MCS-7825-H3 or MCS-7828-H3 servers you cannot revert to the prior version; you must perform a fresh installation.

Related Topics

Refresh upgrade overview, on page 34
Switch version back to Cisco Unified Presence 8.6(3) or earlier, on page 54

Refresh upgrade overview

If required, the server automatically determines if you need to perform a standard upgrade or a refresh upgrade. A refresh upgrade is required when upgrading to IM and Presence from a release earlier than Cisco Unified Presence Release 8.6(4). You can initiate standard and refresh upgrades in the same way using the Command Line Interface or the Cisco Unified IM and Presence Operating System Administration GUI.

A refresh upgrade has the following differences from a standard upgrade:

- multiple reboots as part of the upgrade
- once started, the console displays status information similar to that of a fresh installation
- 16GB USB Flash Drive is required for MCS-7825-H3 and MCS-7828-H3 DRS backup. Do not remove the USB key until the upgrade (data migration) is complete
- COP file installation is required for upgrades from releases 8.0(1) through to 8.6(1)
- different options to switch versions following completion of the upgrade
- e-mail notification is sent upon successful completion of the upgrade

Tip Several reboots will occur during a refresh upgrade, therefore, you must perform a refresh upgrade during a maintenance window.

In a standard upgrade, you are prompted to either **Reboot to upgraded partition** or **Do not reboot after upgrade**. The **Reboot to upgraded partition** option forces a reboot. This option is required to switch the node to the new software release.

In a refresh upgrade, you are prompted to select one of the following options:

- **Switch to new version after upgrade—**no reboot required
- **Do not switch to new version after upgrade—**reboot required

If you want to remain on the upgraded software version, select the **Switch to new version after upgrade** option.

If you want the system to automatically reboot and switch back to the old software version, select the **Do not switch to new version after upgrade** option.

You can select the **Do not switch to new version after upgrade** option to perform a staged upgrade. An example of a staged upgrade would be upgrading a publisher node one night, reverting back to the inactive software, and then switching to the new active software the following night before upgrading the subscriber node(s). In this scenario, you must upgrade all subscriber nodes during the same upgrade window and not switch back the publisher node again. If you switch back the publisher node again, you must follow the procedure to switch to Cisco Unified Presence Release 8.6(3) or earlier.

Related Topics

Version Switching Rules, on page 38
Switch version back to Cisco Unified Presence 8.6(3) or earlier, on page 54

Special considerations for refresh upgrade

Note Cisco highly recommends that you perform a DRS backup before you begin a refresh upgrade.

MCS-7825-H3 or MCS-7828-H3 server upgrade

If an upgrade fails for any server other than an MCS-7825-H3 or MCS-7828-H3 server, you can revert back to the previous software version. However, during an upgrade of an MCS-7825-H3 or MCS-7828-H3 server, the disk is completely reformatted, preventing a switch back to the previous version. As a result, Cisco highly recommends that you have a 16GB USB key to which you can backup the DRS.

You should format the USB key. For more information, see the section covering the Answer File Generator in the *Installation Guide for IM and Presence Service on Cisco Unified Communications Manager*.

COP File Installation

For all upgrades from Cisco Unified Presence Release 8.0.x through Release 8.6(1), you must install a COP file. The name of the COP file is `ciscocm.cup.refresh_upgrade_v<latest_version>.cop` and you can download it from Cisco.com.

Note You must install the COP file on all nodes before you begin the upgrade.

Failing to install the required COP file when necessary results in the following error: “Error encountered: The selected upgrade is disallowed from the current version.” The system aborts the upgrade and automatically reverts back to the previous version of the software. This “COP file check” occurs very early in the upgrade process (preparation phase), prior to the first reboot and reformat of the drive. For more information about the COP file, see Upgrade paths, requirements, and restrictions, on page 37

Refresh upgrade stages

Preparation Phase

The preparation phase of a refresh upgrade occurs immediately after the upgrade is initiated. During this phase, the upgrade progress can be monitored via the GUI or the CLI. After the preparation phase is completed, the server will automatically reboot to continue the upgrade process. The duration of this phase varies depending on the size and the complexity of the database configuration.

Installation Phase

The installation phase of a refresh upgrade is very similar to that of a fresh installation with a few exceptions. The status of this stage can be monitored via the console. No further GUI updates will occur. During this phase, there is no service support.

Note If the upgrade fails on any server other than an MCS-7825-H3 or MCS-7828-H3, the server reboots back to the previous software version and you can inspect the install logs using the Command Line Interface. On an MCS-7825-H3 or MCS-7828-H3 server, the disk is completely reformatted; there is no option to revert to the previous software version. For these servers, Cisco recommends that you dump the diagnostic logs to the USB flash drive.

System Startup Phase

This is the last phase of a refresh upgrade. Following the completion of a refresh upgrade, all IM and Presence applications run the new active software

Upgrade time requirements

The time required to upgrade IM and Presence software is variable and depends on a number of factors, such as the number of users, the average contact list size of each user, whether the upgrade is on the publisher or a subscriber node and the hardware deployed. For large deployments, installation of the upgrade software may take several hours.

Throttling affects time required to upgrade

To preserve system stability during upgrades, the system throttles the upgrade process, which may take considerably longer to complete in Cisco Unified Presence 7.0(1) and later than it did in earlier releases.

Related Topics

Disable throttling, on page 63

License requirements

The IM and Presence Service does not require a server license or software version license. IM and Presence capabilities are integrated with Cisco Unified Communications Manager licenses and are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Refer to the *Cisco Unified Communications Manager Enterprise License Manager User Guide* for more information.

For more information about user license requirements for IM and Presence and Cisco Jabber, see the “Cisco Unified IM and Presence Service installation” section of *Installing Cisco Unified Communications Manager*.

Bridged upgrade

The IM and Presence Service supports bridged upgrades to customers who wish to migrate from discontinued hardware to supported hardware.

The bridged upgrade allows you to create a Disaster Recovery System (DRS) backup on the discontinued hardware. You can then restore the DRS backup on supported hardware after you complete a fresh IM and Presence installation on the supported hardware.

When you attempt an upgrade on the discontinued hardware, IM and Presence displays a warning on the interface, and on the CLI, and informs you that IM and Presence only supports the functionality to create a DRS backup on this server.

IM and Presence supports bridged upgrades from a number of discontinued servers. See the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager* for the list of discontinued servers.

For more information about DRS backups, see the *Disaster Recovery System Administration Guide*.

Upgrade paths, requirements, and restrictions

The following table lists the range of upgrade paths that are supported for the IM and Presence Service. For more detailed information about supported upgrade paths, see the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager* .

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.0(1) to 8.6(1)	9.0(1)	Refresh upgrade, COP file needed
8.6(2) and 8.6(3)	9.0(1)	Refresh upgrade
8.6(4)	9.0(1)	Standard upgrade
Upgrading from Cisco Unified Presence Release 8.6(5) and later to IM and Presence Release 9.0(1) is unsupported.		

For upgrades from Cisco Unified Presence 8.0(1) through to 8.6(1), you must install a COP file on all nodes before you begin the upgrade process. You can download the COP file from Cisco.com. The name of the COP file is:

`cisco.com.cup.refresh_upgrade_v<latest_version>.cop`

The COP file delivers functionality to allow the upgrade path to be supported and provides various enhancements to the user experience.

Caution If you do not install the COP file on all nodes for the required releases, the upgrade will fail.

Software version restrictions

Unified Communications Manager and IM and Presence Service software versions must have the same major and minor release number. Major and minor release numbers are defined as follows:

`9.x.y`

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

For example, IM and Presence Release 9.0.2.10000-4 is compatible with Unified Communications Manager Release 9.0.12.30000-2, but it is not compatible with Unified Communications Manager Release 9.1.1.10000-3. Similarly, Unified Communications Manager Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-9.

The software version of subsequent IM and Presence nodes that you upgrade must match all five version numbers of the first IM and Presence node that you upgraded.

Note You cannot upgrade IM and Presence unless the upgraded release of Unified Communications Manager is already installed on the active or inactive partition. You must upgrade Unified Communications Manager before you can upgrade IM and Presence to the matching version.

Caution If you use Platform Administrative Web Services (PAWS) Management to upgrade IM and Presence, do not attempt to upgrade and reboot to the current IM and Presence release if the active partition on Unified CM is running an incompatible software version. If you do, the upgrade will fail, as expected, but the failure will not be reported until near the end of the upgrade process. You will also experience system downtime when the system reboots.

The delayed upgrade failure notification applies only to upgrades that are performed with PAWS Management. If you perform the upgrade through Cisco Unified IM and Presence Operating System Administration or through the CLI, the upgrade failure notification is displayed at the beginning of the upgrade.

Version Switching Rules

A number of rules apply when you are manually switching versions and when you switch versions during an upgrade.

Manual switching rules

Version Switching During Upgrade Rules

Upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5(4)

If you upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5 to the current release, note the following:

- If you have intercluster peers to Cisco Unified Presence Release 8.0(x) or Release 8.5 clusters, you will not have intercluster presence until you upgrade all of these clusters to Release 8.6 or to Release 9.x and later. After the upgrade is complete, the previously configured peers will start working and intercluster presence will be restored.
- If you upgrade a Cisco Unified Presence Release 8.5 cluster that has High Availability (HA) enabled to Release 9.x or later, Cisco recommends that you disable HA on each subcluster before you begin the upgrade. You can reenable HA on each cluster after the switch version is complete, database replication is complete, and all services are back up and running.
- During a software upgrade, the Cisco Replication Watcher service delays feature service startup on the publisher node for up to 20 minutes and on subscriber nodes indefinitely until replication is established.

User Profile Data Migration

In this release, the user UC Service Profile information for LDAP, Voicemail, Conferencing, Mailstore, CTI Gateway, and Audio that was configured from the **Application** > **CUPC/Cisco Jabber** menu in Cisco Unified Presence Administration is now configurable on Cisco Cisco Unified Communications Manager from the **User Management** > **User Settings** > **UC Service and Service Profile** menus. Therefore, when you upgrade from Cisco Unified Presence Release 8.x to the current release of IM and Presence, all user profile information is migrated to Cisco Unified Communications Manager. The user profile information is stored as new service profiles on Cisco Unified Communications Manager with the following name and description format:

Name: UCServiceProfile_Migration_x (where x is a number starting at 1)

Description: Migrated Service Profile Number x

You can edit these service profiles to give them more meaningful names. See *Cisco Unified Communications Manager Administration Guide* for more information about configuring service profiles.

Note Profiles that have been created on Cisco Unified Presence Release 8.x but have not been assigned to any end users are *not* migrated to Cisco Unified Communications Manager.

The service profiles that are created on Cisco Unified Communications Manager during the user profile data migration include a Presence and IM UC service. The Presence and IM UC service provides Cisco Jabber 9.0 clients with the configuration required to connect to the IM and Presence Service. The Presence and IM UC service is included only in UC service profiles that are assigned to end users.

Note If DNS is not supported in the Cisco Unified Communications Manager deployment, you must modify the **Host Name/IP Address** field for the Presence and IM UC service. When the Presence and IM UC service is created on Cisco Unified Communications Manager, the **Host Name/IP Address** field is set to the IM and Presence domain name. If DNS is not supported, you must change the **Host Name/IP Address** field to the IP address of the IM and Presence publisher node. For more information about configuring UC services, see *Cisco Unified Communications Manager Administration Guide*.

The following examples show how each unique combination of profiles assigned to IM and Presence end users is migrated to Cisco Unified Communications Manager as one new UC service profile.

Figure 1: Example 1

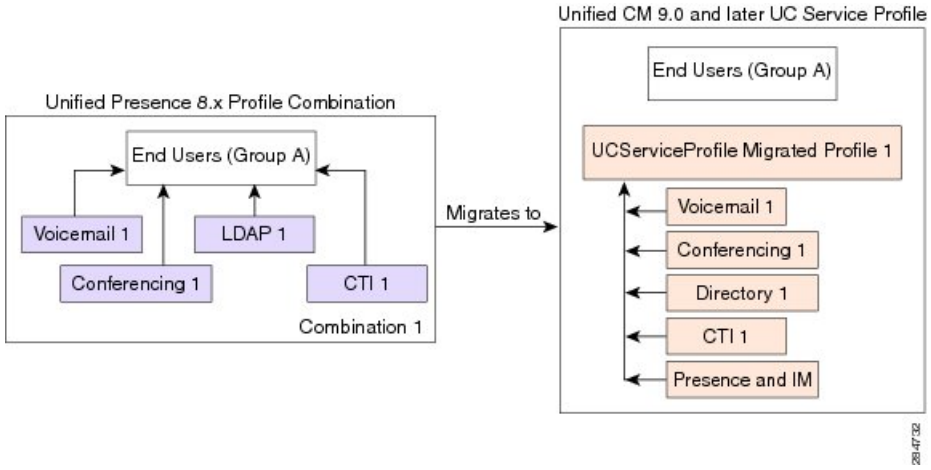


Figure 2: Example 2

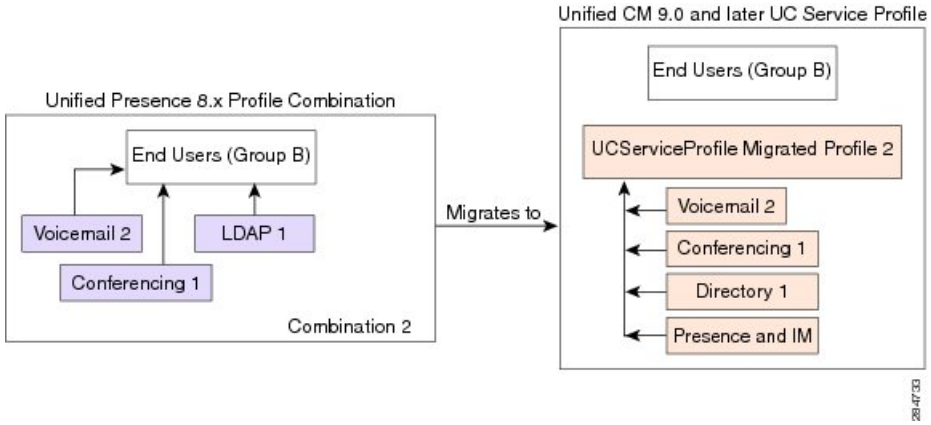
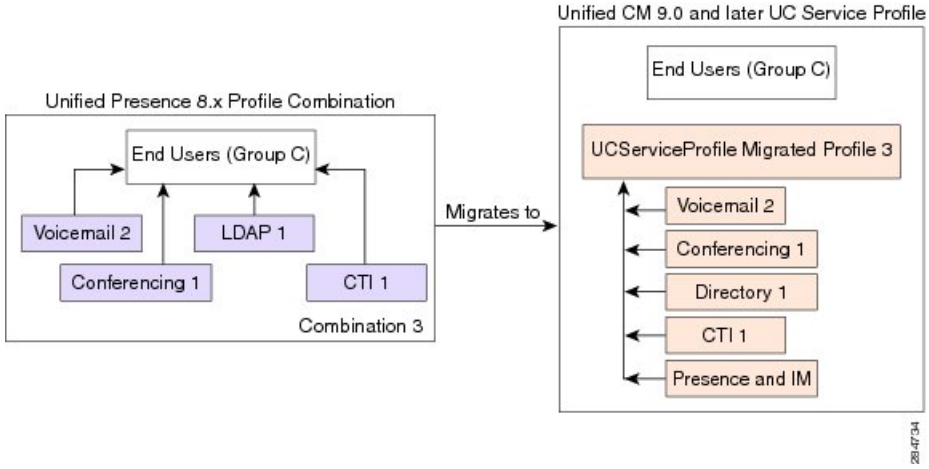


Figure 3: Example 3



Migration of Cisco Jabber Video Settings

In Cisco Unified Presence Release 8.x, the **Always begin with video muted** setting is configured in Cisco Unified Presence Administration under **Application** > **Cisco Jabber** > **Settings**. This setting is not migrated during the upgrade to the current release. In the current release, this setting is configured in Cisco Unified Communications Manager as a Cisco Jabber Enterprise Parameter called **Never start call with video**. The default value for the **Never start call with video** setting is False. If you want to configure calls to not start with video, you must set the **Never start call with video** value to True in the Cisco Unified Communications Manager Enterprise Parameter configuration window.

Intercluster upgrades

This release of the IM and Presence Service supports intercluster peers to clusters running Cisco Unified Presence Release 8.6 and IM and Presence Release 9.x only.

Perform pre-upgrade tasks

Before you begin to upgrade IM and Presence software, you must perform the following tasks.

Procedure

Step 1 Read the release notes and documentation for the new release and be sure you understand the supported upgrades, new features, and how the upgrade interacts with the other products associated with your system.

Step 2 Ensure that your hardware is supported on the version of IM and Presence software that you are upgrading to. See the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager* for more information.

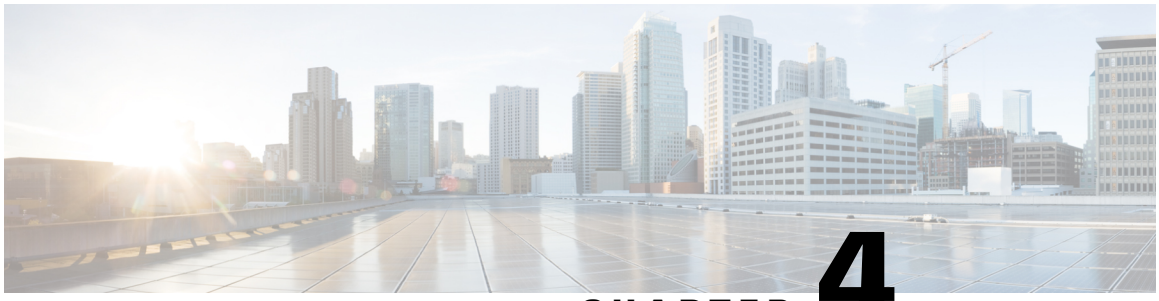
Step 3 Disable High Availability on the IM and Presence subcluster. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology.**
For more information, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 4 Back up your system.
For more information, see the *Disaster Recovery System Administration Guide* .

Step 5 If you have to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop and restart the IM and Presence Sync Agent service. To restart the Sync Agent service, navigate to Cisco Unified IM and Presence Serviceability and select **Tools** > **Control Center - Network Services** .

Step 6 Check that the IM and Presence Service server has connectivity with Cisco Unified Communications Manager.

Tip You can use the Cisco Unified CM IM and Presence Administration System Troubleshooter to check server connectivity.



CHAPTER 4

Upgrade procedures

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

Warning Do not make any changes to IM and Presence configuration during an upgrade. If data is written to the database during the upgrade, the upgrade may fail.

Note If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence server before you attempt another upgrade.

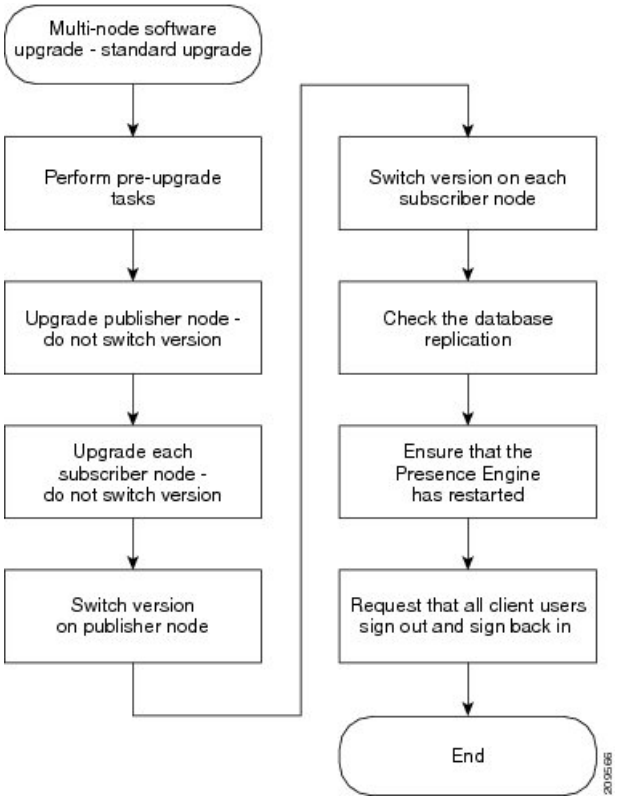
- Multinode software upgrade procedures, page 43
- Software procedures, page 47
- Switch software version, page 52

Multinode software upgrade procedures

This section describes the high-level procedure for performing a standard upgrade and a refresh upgrade in a multinode deployment.

Perform a Standard Upgrade

Figure 4: Multinode Software Upgrade Flowchart - Standard Upgrade



Multinode

Restrictions

Your hardware must comply with the multinode hardware recommendations. See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Server* for more information.

Warning Do not delete any users during the time that you initiate a standard upgrade and switch to the new software version. Deleting users on Cisco Unified Communications Manager (Unified CM) during this time period causes the migration of the UC Profile data from Cisco Unified Presence to Unified CM to fail.

Also, during the time that you initiate a standard upgrade and switch to the new software version, do not perform an LDAP sync that may delete users because this action will cause the migration of the UC Profile data to fail.

Before You Begin

- Check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

- Disable High Availability for IM and Presence Service nodes that are configured for redundancy. For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
- Check that the IM and Presence Service server has connectivity with Cisco Unified Communications Manager.

Attention Perform the pre-upgrade tasks before proceeding.

Procedure

Step 1 Perform pre-upgrade tasks.

Step 2 Upgrade the publisher node. Do not switch the software to the new software release at this point.

Step 3 Upgrade each subscriber node in the cluster. Again, do not switch the software version to the new software release at this point.

Step 4 Switch the software to the new software release on the publisher node. Wait until the publisher node has successfully restarted (is at the sign in prompt) before you proceed to the next step.

Step 5 On the subscriber nodes, switch the software to the new software release.

Step 6 Once the first subscriber has restarted and has come back online with the new software release, switch the software release on the next subscriber node. Wait until each subscriber node has successfully restarted (is at the sign in prompt) before you proceed with the software switch on the next subscriber node. Repeat until the new software release is running on all subscriber nodes.

Step 7 Run the following CLI command to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 8 On each subscriber node, restart the Presence Engine service after the database replication becomes active on the node.

Step 9 Request that all IM and Presence client users in the local and remote cluster sign out, and sign back in to the application.

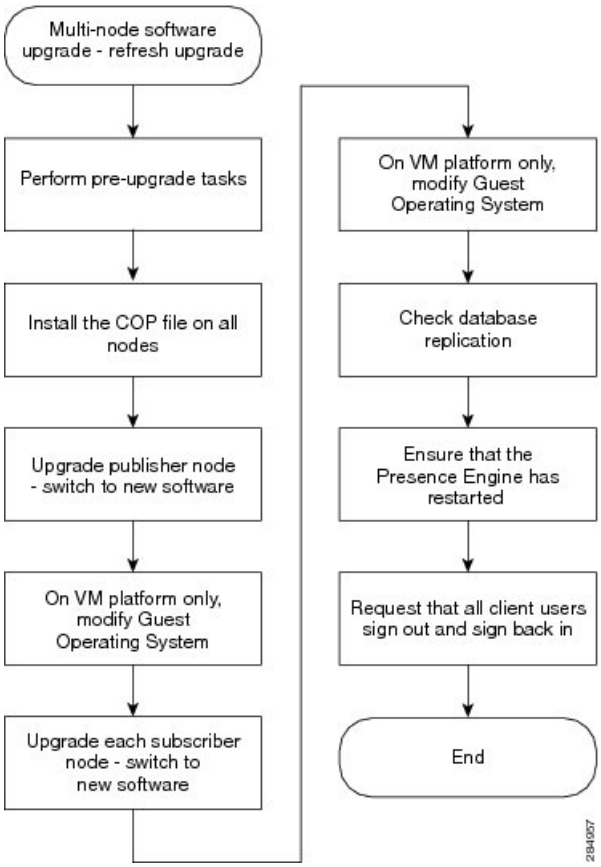
Related Topics

Perform pre-upgrade tasks, on page 41

Perform a Refresh Upgrade

This section describes the high-level procedure to perform a refresh upgrade in a multinode deployment.

Figure 5: Multinode Software Upgrade Flowchart - Refresh Upgrade



Restrictions

Your hardware must comply with the multinode hardware recommendations. See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for more information.

Before you begin

Check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

Procedure

Step 1 Install the following COP file on all nodes in the IM and Presence cluster:
`ciscocm.cup.refresh.upgrade_v<latest_version>.cop`

Step 2 Upgrade the publisher node and switch the software to the new software release. To do this, select **Switch to new version after upgrade**.

Step 3 On VM platforms only, modify the Guest Operating System on the publisher node to Red-Hat Enterprise Linux 5 (32-bit). See the topic on upgrading to a virtual server for more information.

Step 4 Upgrade each subscriber node in the cluster and switch to the new software release by selecting **Switch to new version after upgrade**.

Note The publisher node must be running the new software before you upgrade each subscriber node.

Step 5 On VM platforms only, modify the Guest Operating System on each subscriber node to Red-Hat Enterprise Linux 5 (32-bit). See the topic on upgrading to a virtual server for more information.

Step 6 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on a node:
`utils dbreplication runtimestate`
If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 7 On each subscriber node, restart the Presence Engine service after the database replication becomes active on the node.

Step 8 Request that all IM and Presence client users in the local and remote cluster sign out, and sign back in to the application.

Related Topics

Upgrade to IM and Presence on virtual server, on page 51

Software procedures

You can access the upgrade file during the installation process from either a local CD or DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Note If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence server before you attempt another upgrade.

Related Topics

Upgrade from local source, on page 48

Upgrade from remote source, on page 50
Upgrade to IM and Presence on virtual server, on page 51

Upgrade from local source

You can upgrade to a new release of the IM and Presence Service using software from a CD or DVD in the local disc drive.

Before You Begin

- Obtain the upgrade file from cisco.com. Copy the upgrade file to a writable CD or DVD. Because of their size, some upgrade files may not fit on a CD and require a DVD.
- Review the software upgrade process and ensure that you have completed the prerequisite system backup procedures. Cisco highly recommends that you perform a backup of the Disaster Recovery System (DRS).
- Stop all configuration tasks.
- Perform data migration on MCS-7825-H3 or MCS-7828-H3 servers using a 16GB USB Flash Drive. Do not remove the USB key until the data migration is complete.

Note During a refresh upgrade on either the MCS-7825-H3 or MCS-7828-H3 platform, the hard drive needs to be formatted; it will not be possible to switch back to the older version of Cisco Unified Presence after the refresh upgrade has been started. As a result, Cisco highly recommends that you perform a DRS backup.

- Do not rename the upgrade file before you install it because the system will not recognize it as a valid file.
- Do not decompress the file. If you do, the system may not be able to read the upgrade file.

Tip During a refresh upgrade, traffic is no longer processed and several reboots are required, therefore, you must perform a refresh upgrade during a maintenance window.

Procedure

Step 1 Insert the CD or DVD into the disc drive on the local server that is to be upgraded.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 If you are performing a refresh upgrade, install the required COP file:
`ciscocm.cup.refresh_upgrade_v<latest_version>.cop`

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

Step 5 Select **DVD/CD** from the **Source** list.

Step 6 In the **Directory** field, enter the path to the patch file on the CD or DVD. If the file is in the root directory, enter a slash (/).

Step 7 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This will enable you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 8 Select **Next** to continue the upgrade process.

Step 9 Select the upgrade version that you want to install and select **Next**.

Step 10 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 11 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 12 Perform one of the following actions:
For standard upgrades:

- If this is a single-node deployment and you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**
- If this is a multinode deployment, select **Do not reboot after upgrade.**This allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the topic called *Switch IM and Presence software version*.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you are performing a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note See the topic called *Version switching during upgrade rules* for more information about the rules for switching during an upgrade.

Step 13 Select **Next** and select **Finish** when the installation completes.

Related Topics

Switch software version, on page 52
Version Switching During Upgrade Rules, on page 38

Upgrade from remote source

You can upgrade IM and Presence using software from a network drive or remote server. The network drive or remote server must be running a SFTP/FTP server that can be accessed by each IM and Presence server that you want to upgrade.

Before You Begin

- Review the software upgrade process and ensure that you have completed the prerequisite system backup procedures. Cisco highly recommends that you perform a backup of the Disaster Recovery System (DRS).
- Stop all configuration tasks.
- Perform data migration on MCS-7825-H3 or MCS-7828-H3 servers using a 16GB USB Flash Drive. Do not remove the USB key until the data migration is complete.

Note During a refresh upgrade on either the MCS-7825-H3 or MCS-7828-H3 platform, the hard drive needs to be formatted; it will not be possible to switch back to the older version of Cisco Unified Presence after the refresh upgrade has been started. As a result, Cisco highly recommends that you perform a DRS backup.

Tip During a refresh upgrade, traffic is no longer processed and several reboots are required, therefore, you must perform a refresh upgrade during a maintenance window.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 2 If you are upgrading from a Release between 8.0(1) and 8.6(1) install the required COP file:
`ciscocm.cup.refresh_upgrade_v<latest_version>.cop`

Step 3 Select **Software Upgrades** > **Install/Upgrade**.

Step 4 Select **Remote Filesystem** from the **Source** list.

Step 5 In the **Directory** field, enter the path to the patch file on the remote system.

Step 6 In the **Server** field, enter the FTP or SFTP server name.

Step 7 In the **User Name** field, enter the user name for the remote server.

Step 8 In the **User Password** field, enter the password for the remote server.

Step 9 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This will enable you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 10 From the **Transfer Protocol** field, select the transfer protocol, for example, SFTP.

Step 11 Select **Next** to continue the upgrade process.

Step 12 Select the upgrade version that you want to install and select **Next**.

Step 13 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 14 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 15 Perform one of the following actions:
For standard upgrades:

- If this is a single-node deployment and you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**
- If this is a multinode deployment, select **Do not reboot after upgrade.**This allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the topic called *Switch IM and Presence software version*.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you are performing a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note See the topic called *Version switching during upgrade rules* for more information about the rules for switching during an upgrade.

Step 16 Select **Next** and select **Finish** when the installation completes.

Related Topics

Switch software version, on page 52
Version Switching During Upgrade Rules, on page 38

Upgrade to IM and Presence on virtual server

Follow this procedure if you want to upgrade to IM and Presence Release 9.x and later on a virtual server.

Before you begin

The following components of the virtual server must meet the requirements for the latest release of IM and Presence:

- Guest Operating System
- RAM
- Red Hat Enterprise Linux (RHEL) version 5.0

For information about installing or upgrading IM and Presence on a virtual server, see the Virtualization Docwiki at http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.

Procedure

Step 1 Upgrade the IM and Presence server to the latest software version.

Step 2 After you finish the upgrade, shut down the virtual machine.

Step 3 Change the Guest Operating System to Red-Hat Enterprise Linux 6.0 (32-bit).

Step 4 Compare the Virtual Machine settings on each node to be upgraded with the OVA template for the target upgrade release and the number of users for the node. In particular, compare the following settings:

- number of CPUs
- reserved CPU MHz
- RAM size
- RAM reservation
- number and size of hard disk

For more information about OVA template details, see the Virtualization Docwiki at http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.

Step 5 Save the changes.

Step 6 Restart the virtual machine.

Switch software version

Caution This procedure causes the system to restart and become temporarily out of service.

When you upgrade software, the new software is installed as an inactive version. You can reboot to the new software during the upgrade process or you can switch to the new version later.

When you switch versions, the system restarts, and the inactive software becomes active. The system restart may take up to 15 minutes. When you perform this procedure both the active and inactive software versions are indicated.

Note If you switch versions in a multinode deployment, you must switch the publisher node first. It may take some time for all the services on the IM and Presence nodes to move to the Started state. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology** and select a node from the tree view to monitor the status of the services on the node.

Before You Begin

The software versions on Cisco Unified Communications Manager (Unified CM) and IM and Presence must match according to the manual switching rules. Therefore, you must switch Unified CM before you switch IM and Presence.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Settings** > **Version**.
Step 3 Verify the version of the active software and the inactive software.
Step 4 Select **Switch Versions** to switch versions and restart the system.

Related Topics

Manual switching rules, on page 38

Revert to previous software version

Caution This procedure causes the system to restart and become temporarily out of service.

After you upgrade IM and Presence to a new software version, the earlier software version remains inactive on the system. If you need to revert to the earlier software version, you can switch versions. If you want to switch to Cisco Unified Presence Release 8.6(3) or earlier, see the relevant topic.

Caution You cannot revert to the earlier software version on an MCS-7825-H3 or MCS-7828-H3 server. The entire disk has been reformatted and old data has been erased.

Note Any changes you made to the database after an upgrade will be lost if you revert to the earlier software version. Therefore, if you make changes to the database after an upgrade, you must repeat those changes after you switch back to the earlier software version.

Before you begin

Switch versions on Cisco Unified Communications Manager, see the topic on manual switching rules for more information.

Procedure

Step 1 Sign in to Cisco Unified IM and Presence Operating System Administration.
Step 2 Select **Settings** > **Version**.
Step 3 Verify the version of the active and inactive software.
Step 4 Select **Switch Versions** to switch versions and restart the system.

Related Topics

Switch version back to Cisco Unified Presence 8.6(3) or earlier, on page 54
Manual switching rules, on page 38

Switch version back to Cisco Unified Presence 8.6(3) or earlier

Cisco Unified Presence releases 8.6(4) and later do not support the Cisco Presence Engine database. If you upgrade from Release 8.6(3) or earlier and you subsequently want to revert to the previous release, you must install a COP file that will reinstall the Cisco Presence Engine database. The COP filename is `ciscocm.cup.pe_db_install.cop` and you can download it from Cisco.com.

Note In a multinode environment, you must install the COP file on every node in the cluster after you switch versions from Cisco Unified Presence Release 8.6(4) or later.

The COP file can only be installed on the following versions of Cisco Unified Presence after a downgrade from IM and Presence Release 8.6(4) or later:

- 8.0(1)
- 8.0(2)
- 8.0(3)
- 8.0(4)
- 8.5(1)
- 8.5(2)
- 8.5(3)
- 8.5(4)
- 8.6(1)
- 8.6(2)
- 8.6(3)

Note You must restart the system after you install the COP file.

Before you begin

Switch versions on Cisco Unified Communications Manager.

Procedure

Step 1 Download the following COP file from Cisco.com: `ciscocm.cup.pe_db_install.cop`.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 Select **Settings** > **Version**.

Step 4 Verify the version of the active and inactive software.

Note This procedure only applies if you want to switch from Release 9.0 or later back to a release earlier than 8.6(4).

Step 5 Select **Switch Versions** to switch back to the earlier release and restart the system.

Step 6 After the system has restarted, install the COP file.

Note In a multinode environment, you must install the COP file on every node in the cluster.

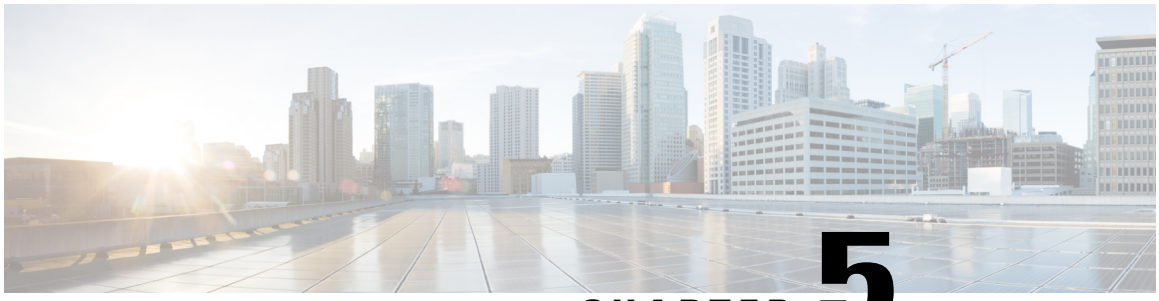
Step 7 After you have installed the COP file, manually restart the system. To do this, select **Settings** > **Version** and select **Restart**.

Step 8 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on the node: `utils dbreplication runtimestate`

If database replication is active on all nodes, the output lists all the nodes and the replication setup value for each node is 2. If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete.

Step 9 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 10 If database replication cannot be established, use the following CLI command on the publisher node to reset replication: `utils dbreplication reset all`



CHAPTER 5

Post-upgrade tasks

This section describes the post-upgrade tasks for the IM and Presence Service.

- High Availability, page 57
- Verify IM and Presence Service Data Migration, page 57

High Availability

If your deployment supports high-availability, you must turn high-availability back on in each subcluster. Do this after you switch versions, finish the database replication and restart all services. For information about how to turn on high-availability, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Verify IM and Presence Service Data Migration

When you upgrade from Cisco Unified Presence Release 8.x to IM and Presence Service Release 9.x and later, user profiles are migrated to Cisco Cisco Unified Communications Manager. The user profile information is stored as new service profiles on Cisco Unified Communications Manager with the following name and description format:

Name: UCServiceProfile_Migration_x (where x is a number starting at 1)

Description: Migrated Service Profile Number x

To ensure that users can successfully log into Cisco Jabber after an upgrade from Cisco Unified Presence Release 8.x, you must verify that the user profile data migration was successful.

Profiles that are created but that are not assigned to users are *not* migrated to Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, select **User Management** > **User Settings** > **Service Profile**.

Step 2 Select **Find** to list all service profiles.

Step 3 Verify that there are migrated service profiles with the following name format: *UCServiceProfile_Migration_x*

Step 4 If there are no migrated service profiles, check the `installdb log` file for any errors.

Step 5 If there is an import error, an alarm is raised on Cisco Unified Communications Manager. To view the alarm details, log into RTMT for Cisco Unified Communications Manager.

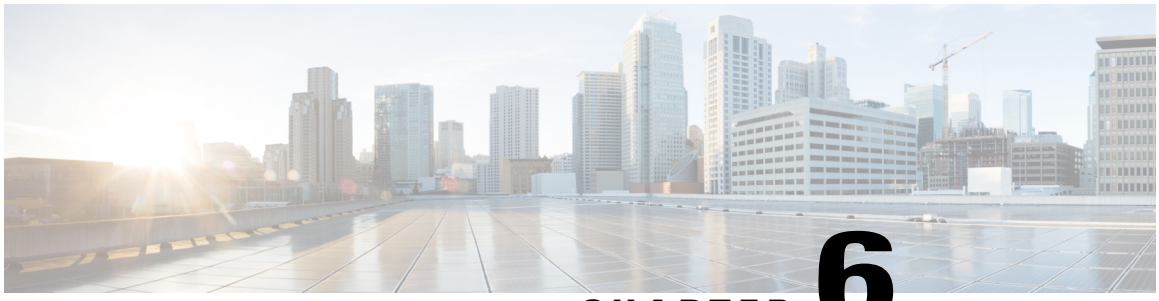
What to Do Next

You can edit these service profiles to give them more meaningful names. See *Administration Guide for Cisco Unified Communications Manager* for more information about configuring service profiles.

For more information about how user profiles are migrated, see the section “User profile data migration”.

Related Topics

User Profile Data Migration, on page 39



CHAPTER 6

Troubleshooting

The following chapter contains troubleshooting information about the IM and Presence Service.

- IM and Presence user phone presence problems, page 59
- Presence User Experiences Issues Obtaining Availability, page 59
- Real-Time Monitoring Tool alert for Cisco SIP proxy service, page 60
- Cannot find upgrade file on remote server, page 60
- Upgrade file checksum values do not match, page 60
- Database replication did not complete, page 60
- Cisco UP Presence Engine database does not restart, page 60
- Version Errors, page 61
- Failed refresh upgrade, page 61
- Cancelled or failed upgrade, page 61
- Upgrade From Pre Release 8.6(4) Fails, page 61
- Directory Was Located and Searched but No Valid Options or Upgrades Were Available, page 62

IM and Presence user phone presence problems

Problem After an IM and Presence server upgrade, when all activated feature services and network services are started, IM and Presence phone presence from users is delayed or slow to update.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Presence User Experiences Issues Obtaining Availability

Problem After an IM and Presence Service server upgrade, when all activated feature services and network services are started, a user experiences inconsistent presence availability. The user can log in to IM and Presence Service but experiences issues obtaining availability information mainly from SIP-based clients.

Solution This issue is caused when users are provisioned while IM and Presence Service is being upgraded. You must unassign and then reassign the user.

Real-Time Monitoring Tool alert for Cisco SIP proxy service

Problem After an IM and Presence server upgrade, when all activated feature services and network services are started, a Real-Time Monitoring Tool CoreDumpFileFound alert was generated for the Cisco SIP Proxy service.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Cannot find upgrade file on remote server

Problem You cannot find the upgrade file on the remote server.

Solution 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 that you want to specify. 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, check with your system administrator for the correct directory path.

Upgrade file checksum values do not match

Problem The checksum value of the upgrade file does not match the checksum indicated on Cisco.com.

Solution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Database replication did not complete

Problem After an upgrade, database replication did not complete and the result of the command **`utils dbreplication runtimestate`** was not 2.

Solution After a successful upgrade and switch version to the new software, database replication should take place automatically. During this time core services on the subscriber nodes will not start. Database replication in large deployments can take several hours to complete. If, after several hours, the **`utils dbreplication runtimestate`** command shows that database replication did not complete, you need to reset the database replication. Run the following command on the publisher node: `utils dbreplication reset all`

Cisco UP Presence Engine database does not restart

Problem After you switch back to Cisco Unified Presence Release 8.6(3) or an earlier software version, the Cisco UP Presence Engine database does not restart.

Solution Ensure that you installed the required COP file, `ciscocm.cup.pe_db_install.cop`, on every node in the cluster after you switched back to Cisco Unified Presence Release 8.6(3), or earlier.

Version Errors

Selected Upgrade Is Disallowed From the Current Version

Problem During a refresh upgrade, the following error is reported: `Error encountered: The selected upgrade is disallowed from the current version`.

Solution You did not install the required COP file on the node. Download the following COP file from Cisco.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`. Restart the server. Install the COP file on every node in the cluster before you attempt the refresh upgrade again.

Failed refresh upgrade

Problem A refresh upgrade failed.

Solution Restart the system, it should reboot to the software version that was running before you attempted the refresh upgrade. If you cannot access the system, you must use the Recovery CD to recover the node.

Cancelled or failed upgrade

If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence server before you attempt another upgrade.

Upgrade From Pre Release 8.6(4) Fails

Problem You are upgrading from a release earlier than Cisco Unified Presence 8.6(4) and the upgrade fails on both the publisher and subscriber nodes.

Solution The Cisco Unified Communications Manager hostname is case-sensitive. You must ensure that the entry for the Cisco Unified Communications Manager publisher node on the Cisco Unified Presence Administration interface matches exactly the Cisco Unified Communications Manager hostname. Complete the following procedure:

1. Log into **Cisco Unified Presence Administration** interface and choose **System** > **CUCM Publisher**.
2. If the **CUCM Publisher Hostname** value does not match the hostname, modify it and click **Save**.
3. Restart the Cluster Manager service with the following CLI command: **utils service restart Cluster Manager**
4. Open the platformConfig.xml file at the following location: `/usr/local/platform/conf/`
5. Verify that the values for *IPSecMasterHost* and *NTPServerHost* match exactly the Cisco Unified Communications Manager hostname.

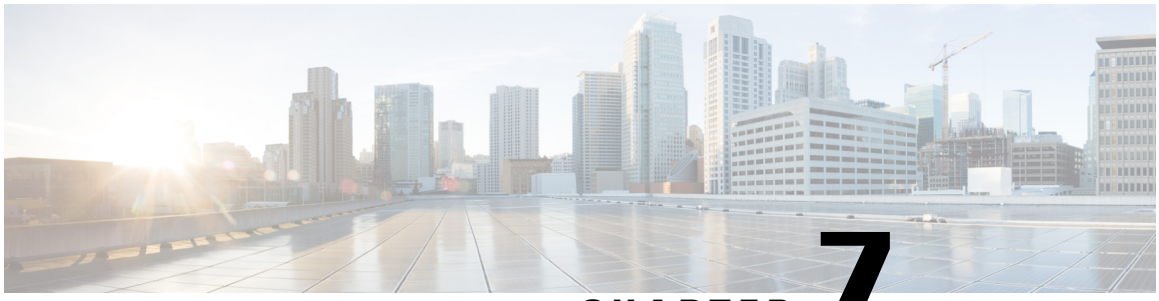
6 If necessary, modify the value for *IPSecMasterHost* and *NTPServerHost* , save the platformConfig.xml file and restart the Cluster Manager service again.

Directory Was Located and Searched but No Valid Options or Upgrades Were Available

Problem During an IM and Presence Service upgrade, the IM and Presence Service server generates the following error message, even though the upgrade path and file are valid:

```
The directory was located and searched but no valid options or upgrades
were available. Note, a machine cannot be downgraded so option and upgrade
files for previous releases were ignored.
```

Solution The upgrade manager checks for connectivity between IM and Presence Service and Cisco Unified Communications Manager to validate the version during the upgrade. If this fails, the IM and Presence Service server generates the error message even though the upgrade path and file are valid. Use a tool, such as the Cisco Unified CM IM and Presence Administration System Troubleshooter, to check that there is connectivity between IM and Presence Service and Cisco Unified Communications Manager before proceeding with the upgrade.



CHAPTER 7

Reference

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

- Effects of I/O throttling, page 63
- Locale specific upgrades, page 66

Effects of I/O throttling

Overview

This section describes how throttling affects the upgrade process, identifies possible causes of slow or stalled upgrades, and provides actions you can take to speed up the upgrade.

Throttling may cause the upgrade to take longer. Throttling is enabled by default and is necessary if you perform the upgrade during normal business hours.

Disable throttling

To disable throttling, use the following command in the CLI before you start the upgrade:

```
utils iothrottle disable
```

Note If you want to restart throttling after you start the upgrade, you must cancel the upgrade, restart throttling, and then restart the upgrade.

Server models

The Server model you have also impacts the upgrade speed. Upgrades on servers that have SATA hard drives, such as MCS-7816 and MCS-7825, take longer than servers with SAS/SCSI hard drives, such as MCS-7835 and MCS-7845.

Write-cache

A disabled write-cache on the server also causes the upgrade process to run more slowly. Multiple factors can cause the write-cache to become disabled, including dead batteries on older servers.

Before starting an upgrade, verify the status of the write-cache on the MCS-7835/45 disk controllers. You do not need to verify the write-cache status on the MCS-7816, MCS-7825 servers. To verify write-cache status, access the Cisco Unified IM and Presence Operating System Administration, and select **Show > Hardware**.

If you determine that your write-cache is disabled because of a dead battery, you need to replace the hard disk controller cache battery. Follow your local support procedures to get this battery replaced.

See the following examples of output from the **Show > Hardware** menu for details on determining the battery and write-back cache status.

In the following example write-cache is enabled. The example indicates that 50 percent of the cache is reserved for write and 50 percent of the cache is reserved for read. If the write-cache was disabled, 100 percent of the cache would be reserved for read or the Cache Status would not equal “OK”. Also, the battery count equals “1”. If the controller battery was dead or missing, it would indicate “0”.

7835/45-H1 and 7835/45-H2 Servers with Write-Cache Enabled

```
------------------------------RAID Details      :

Smart Array 6i in Slot 0
   Bus Interface: PCI
   Slot: 0
   Cache Serial Number: P75B20C9SR642P
   RAID 6 (ADG) Status: Disabled
   Controller Status: OK
   Chassis Slot:
   Hardware Revision: Rev B
   Firmware Version: 2.80
   Rebuild Priority: Low
   Expand Priority: Low
   Surface Scan Delay: 15 sec
   Cache Board Present: True
   Cache Status: OK
   Accelerator Ratio: 50% Read / 50% Write
   Total Cache Size: 192 MB
   Battery Pack Count: 1
   Battery Status: OK
   SATA NCQ Supported: False
```

The following example indicates that the battery status is enabled and that the write-cache mode is enabled.

7835/45-I2 Servers with Write-Cache Enabled

```
----------RAID Details      :
Controllers found: 1

---------------------------------------------------------------------
Controller information
---------------------------------------------------------------------
   Controller Status                    : Okay
   Channel description                  : SAS/SATA
   Controller Model                     : IBM ServeRAID 8k
   Controller Serial Number             : 20ee0001
   Physical Slot                        : 0
   Copyback                             : Disabled
   Data scrubbing                       : Enabled
   Defunct disk drive count             : 0
   Logical drives/Offline/Critical      : 2/0/0
   ------------------------------------------------
   Controller Version Information
```

```
   ------------------------------------------------
   BIOS                                : 5.2-0 (15421)
   Firmware                            : 5.2-0 (15421)
   Driver                              : 1.1-5 (2412)
   Boot Flash                          : 5.1-0 (15421)
   ------------------------------------------------
   Controller Battery Information
   ------------------------------------------------
   Status                              : Okay
   Over temperature                    : No
   Capacity remaining                  : 100 percent
   Time remaining (at current draw)    : 4 days, 18 hours, 40 minutes
   ------------------------------------------------
   Controller Vital Product Data
   ------------------------------------------------
   VPD Assigned#                       : 25R8075
   EC Version#                         : J85096
   Controller FRU#                     : 25R8076
   Battery FRU#                        : 25R8088

---------------------------------------------------------------------
Logical drive information
---------------------------------------------------------------------
Logical drive number 1
   Logical drive name                  : Logical Drive 1
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,0 0,1
Logical drive number 2
   Logical drive name                  : Logical Drive 2
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,2 0,3
```

7845/45-I3 Servers with Write-Cache Enabled

```
HW Platform       : 7845I3Processors        : 2
Type              : Intel(R) Xeon(R) CPU           E5540  @ 2.53GHz
CPU Speed         : 2530
Memory            : 8192 MBytes
Object ID         : 1.3.6.1.4.1.9.1.587
OS Version        : UCOS 4.0.0.0-44
Serial Number     : KQNDPGG

RAID Version      :
Raid firmware version: 11.0.1-0024

BIOS Information  :
IBMCorp. -[D6E145FUS-1.07]- 04/26/2010
...
...
Logical Drives Information:
==========================
Virtual Disk: 0 (Target Id: 0)
Name:
RAID Level: Primary-1, Secondary-0, RAID Level Qualifier-0
Size:278.464 GB
State: Optimal
Stripe Size: 128 KB
Number Of Drives:2
Span Depth:1
Default Cache Policy: WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
```

```
Current Cache Policy: WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
Access Policy: Read/Write
Disk Cache Policy: Disk's Default
Encryption Type: None
Virtual Disk: 1 (Target Id: 1)
Name:
RAID Level: Primary-1, Secondary-0, RAID Level Qualifier-0
Size:278.464 GB
State: Optimal
Stripe Size: 128 KB
Number Of Drives:2
Span Depth:1
Default Cache Policy: WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
Access Policy: Read/Write
Disk Cache Policy: Disk's Default
Encryption Type: None

...
...
```

Locale specific upgrades

About Locales

Cisco provides locale-specific versions of the IM and Presence Locale Installer on www.cisco.com. The locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

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

When installing IM and Presence locales, you must install the user locale files, which contain language information for a specific language and country and use the following naming convention:

```
ps-locale-language-country-version.cop
```

Locale installation

Note Before you install a locale for a country on IM and Presence, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. You must restart each server in the cluster after installation to activate the new locales. For more information about installing locales, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

INDEX

D

dial plan installation 23

E

error messages 25
  descriptions 25

I

installing 23, 66
  dial plan 23
  locales 23, 66

L

locales 23, 24, 25, 66
  files 24
  installation 23, 66
  installer 25
    error messages 25
  installing 66

M

messages 25
  error 25

S

software 15, 16, 17, 18, 47, 48, 50
  installation 47
  upgrades 15, 16, 17, 18, 47, 48, 50
    bridge upgrade 18
    from local source 15, 48
    from remote source 16, 17, 50
    procedure 47
supported products 26

T

TFTP server 26
  installing files 26