Cisco Prime Collaboration Deployment Administration Guide, Release 11.5(3)

First Published: August 24, 2016

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

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

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

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

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

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

Introduction to Cisco Prime Collaboration Deployment 1

CHAPTER 2 **Install Cisco Prime Collaboration Deployment** 3

System Requirements for Installation 3

Browser Requirements 4

IP Address Requirements 4

Virtualization Software License Types 4

Frequently Asked Questions About the Installation 5

Preinstallation Tasks 6

Begin Installation 14

Install Cisco Prime Collaboration Deployment 14

Extract the PCD_VAPP.OVA File 14

Install the Virtual Machine 15

Configure Cisco Prime Collaboration Deployment on the Virtual Machine 16

Postinstallation Tasks 18

CHAPTER 3 **Upgrade Cisco Prime Collaboration Deployment** 19

Upgrade Cisco Prime Collaboration Deployment Using CLI 19

CHAPTER 4 **Cisco Prime Collaboration Deployment Features** 21

Cisco Prime Collaboration Deployment Considerations 21

Network Address Translation Support 23

Configure Cisco Prime Collaboration Deployment Behind the NAT 23

Supported Tasks for Applications and Versions 24

Upgrade Paths for Export Restricted and Unrestricted Software 28

Supported ESXi Server Versions 28

Cluster Inventory 29

Discover a Cluster 29
Modify and View a Cluster 31
Add an ESXi Host Server 32
Create a Migration Cluster 32
Add New Cluster for Fresh Install 34
Task Management 35
Migration Task 36
Before You Begin 36
Create a Migration Task 37
Run a Migration Task 39
Postmigration Tasks for Cisco Unified Communication Manager Nodes in the Cluster 40
Post Migration Tasks for IM and Presence Service 41
Migration Procedure Flow Charts 42
Simple Migration 43
Pre Release 8.0.1 Unified CM Network Migration 44
Release 8.0.1 And Later Unified CM Network Migration 45
Recovery of Original Cluster 46
Check the Status of the Cluster Manager Service on All Source Nodes 46
Upgrade Task 47
Create an Upgrade Task 47
Reuse Sequence from Previous Task 50
Switch Versions Task 50
Create a Switch Versions Task 50
Server Restart Task 53
Create a Server Restart Task 53
Readdress Task 55
Create a Readdress Task 55
Run a Readdress Task 56
Post Readdress Task 57
Install Task 57
Create an Install Task 57
Add Install Task 58
Run an Install Task 60
Cancel Install Task 61

Post-Install Task 61
Edit and Expand Cluster Support 61
Edit or Delete a New Install Cluster 61
Edit or Delete a Discovered Cluster 62
Monitor Task Status 63
Action Buttons on the Monitoring Page 64
Automatic Refresh 65
Administration Tools 65
Email Notification 65
When Email Is Sent 65
SFTP Datastore 66
Migration or Fresh Install Tasks 66
Upgrade Task 66
Verify or View an ISO Filename 67
Delete ISO or COP Files 67
Remote SFTP Server Support 68
Add Remote SFTP server 68
Associate Nodes to Remote SFTP Server 69
Edit Remote SFTP Server 70
Delete Remote SFTP Server 70
Delete Local SFTP/Datastore ISO files 71
Disk Space Warning Level 71
Configure Disk Space Warning Level 72
Audit Log Configuration 72
Configure Audit Logs 72
Customized Logon Message 73
Configure Customized Logon Message 73
FIPS 140-2 Compliance 74
EnhancedSecurityMode Support 74
Credential Policy for EnhancedSecurityMode 75
EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment 75
Audit Framework and Audit Activities 75
EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment 76

Re-encryption through AES 76
Limited Number of Sign-in Sessions 77

CHAPTER 5 Cisco Prime Collaboration Deployment Administrative Interface Elements 79
Common Administrative Interface Elements 79
Monitoring View Elements 80
Tasks View Elements 84
Upgrade View 84
Switch Versions View 88
Server Restart View 93
Readdress View 98
Install View 104
Migrate View 108
Inventory View Elements 113
Clusters 113
ESXi Hosts View 120
SFTP Servers and Datastore 121
Administration View Elements 122
Email Notification View 122
NAT Settings 124
Disk Space Warning Level 125
Audit Log Configuration 125
Customized Logon Message Configuration 127

CHAPTER 6 Cisco Prime Collaboration Deployment Configuration and Administration 129
Services 129
Limitations and Restrictions 133

CHAPTER 7 CLI Commands and Disaster Recovery System 135
CLI Commands on Cisco Prime Collaboration Deployment 135
Create a DRS Backup of the Server 137
Important Notes on Backup and Restore 138
Restore a Backup to Cisco Prime Collaboration Deployment 138

CHAPTER 8 CLI Commands for EnhancedSecurityMode and FIPS Mode 141

CLI Commands for EnhancedSecurityMode 141
Configure EnhancedSecurityMode 141
CLI Commands for FIPS Mode 142
Enable FIPS Mode 142
Disable FIPS Mode 143
User Account and Sign-in Attempts on CLI and Interface 144
Configure Remote Audit Logging for Platform Logs 144
Configure Logstash Server Information 145
Configure the FileBeat Client 145
Platform CLI Commands for Security in EnhancedSecurityMode 146

CHAPTER 9 CTL Update 149
More Information 149
Bulk Certificate Management 149

CHAPTER 10 Best Practices 151
Cluster Discovery 151
Upgrades 152
ESXi Host 152
Migration and Installation Virtual Machines 152
Premigration 152
Check TFTP Directory Disk Usage 153
Delete TFTP Files 153
Postmigration 153
Task Validation 154
Cisco Prime Collaboration Deployment Shutdown 154
Monitoring Tasks 154
Managing Files in the SFTP Datastore 154
Using Cisco Prime Collaboration Deployment with Clustering Over WAN 155
Sequence During Migration 155
Server Readdress 155
Fresh Install Publishers and Subscribers 155
Fresh Install of a Unified CM and IM and Presence Cluster 155
Email Notification 156
Test Email 156

CHAPTER 11 Cisco Prime Collaboration Deployment Troubleshooting 157

Increase Disk Space for Migrations 157

General Troubleshooting Issues 158

Errors Seen in View Log 158

Lock Errors 162

NFS Datastores 162

Pause States on Monitor Page 162

Scheduling 163

Server Connectivity 163

Task Failure Due to Restart 163

Installation Task Failure 164

Upgrade Task Failure 165

Migration Task Failure 167

Switch Version Task Failure 168

Readdress Task Failure 169

Server Restart Task Failure 171

Task Scheduling 172

Task Timeouts 173

Upgrade Migration and Installation 173

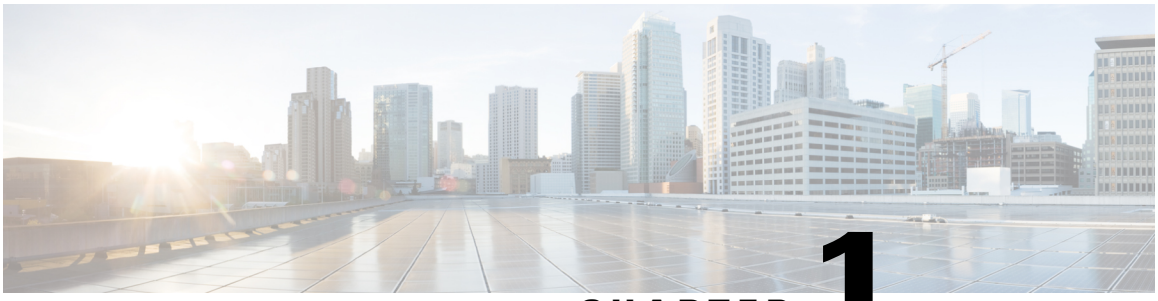
Run a New Task When Current Task in Canceling State 174

Rerun Fresh Install Task 174

Rerun Migration Task 175

Version Validity 175

ISO File Does Not Get Loaded Or Not Recognized During Migration 176



CHAPTER 1

Introduction

- Introduction to Cisco Prime Collaboration Deployment, page 1

Introduction to Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications (UC) applications. It allows you to perform tasks such as migration of older software versions of clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

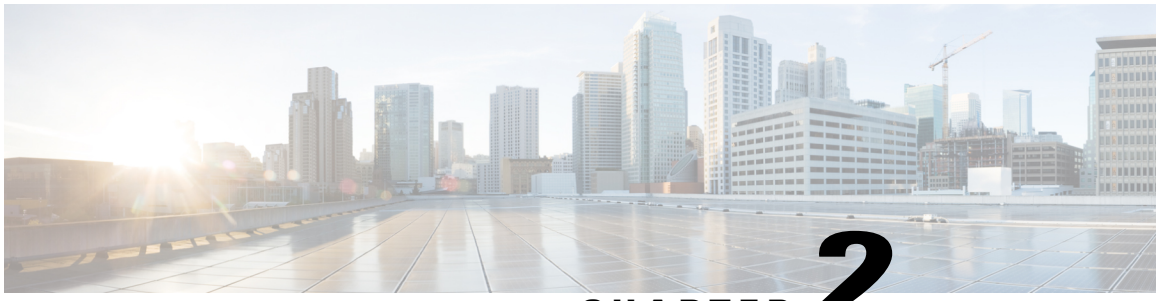
Cisco Prime Collaboration Deployment has four primary high-level functions:

- Migrate an existing cluster of UC servers to a new cluster (such as MCS 7800 to virtual or virtual to virtual)
- Perform operations on existing clusters (8.6(1) or later). Examples of these operations include:
  - Upgrade
  - Switch version
  - Restart
- Change IP addresses or hostnames in the cluster on existing Release 10.x clusters.

Important All the IP addresses that are mentioned in this document applies only for the IPv4 address format.

- Fresh install a new Release 10.x or 11.x Unified Communications cluster

Note Cisco Prime Collaboration Deployment features are only supported by specific software versions. For details on software versions that are compatible with each Cisco Prime Collaboration Deployment feature, see Supported Tasks for Applications and Versions, on page 24. For details on supported upgrade paths, see Upgrade Paths for Export Restricted and Unrestricted Software, on page 28.



CHAPTER 2

Install Cisco Prime Collaboration Deployment

- System Requirements for Installation, page 3
- Browser Requirements, page 4
- IP Address Requirements, page 4
- Virtualization Software License Types, page 4
- Frequently Asked Questions About the Installation, page 5
- Preinstallation Tasks, page 6
- Begin Installation, page 14
- Install Cisco Prime Collaboration Deployment, page 14
- Postinstallation Tasks, page 18

System Requirements for Installation

As defined in the open virtualization format (OVA) that you must use to install Cisco Prime Collaboration Deployment, the following are the server requirements.

Table 1: Cisco Prime Collaboration Deployment Installation Server Requirements

Requirement	Notes
Product	Cisco Prime Collaboration Deployment
Version	11.5(3)
CPU	2 vCPUs
Memory	4 GB
Hard Drive	80 GB (one)
Licensing	Cisco Prime Collaboration Deployment does not require a license

Browser Requirements

Cisco Prime Collaboration Deployment provides a GUI interface that you can use to configure and manage the system. You can access the interfaces by using the browsers and operating systems listed here.

Note Other browsers are not supported.

Cisco Prime Collaboration Deployment supports the following operating system browsers:

- Mozilla Firefox 42
- Mozilla Firefox ESR 38.4
- Google Chrome 46
- Microsoft Internet Explorer (IE) 9, 10, 11
- Apple Safari 7

From any user PC in your network, browse to a server that is running Cisco Prime Collaboration Deployment and log in with administrative privileges.

Note Simultaneous login to Cisco Prime Collaboration Deployment Administration GUI by more than five users can affect performance. Limit the number of users and administrators that are logged in simultaneously.

Note Cisco Prime Collaboration Deployment Administration does not support the buttons in your browser. Do not use the browser buttons (for example, the Back button) when you perform configuration tasks.

IP Address Requirements

You must configure the Cisco Prime Collaboration Deployment server to use static IP addressing to ensure that the server obtains a fixed IP address.

Virtualization Software License Types

The VMware vSphere ESXi license is required for the physical server with ESXi that hosts the Cisco Prime Collaboration Deployment virtual machine in addition to any additional physical servers with ESXi on which Cisco Prime Collaboration Deployment will operate. This includes virtual machines to which Cisco Prime Collaboration Deployment is migrating, installing, upgrading, or rebooting.

Cisco Prime Collaboration Deployment is not compatible with all license types of VMware vSphere ESXi, because some of these licenses do not enable required VMware APIs.

Note Cisco Business Edition 6000 and Cisco Business Edition 7000 servers, which are originally shipped with Cisco Collaboration Systems Release (CSR) 11.0 or older software preload, are preinstalled with Cisco UC Virtualization Hypervisor. If you plan to use Cisco Prime Collaboration Deployment with application VMs on these servers, you must substitute a higher virtualization software feature level.

The following are compatible with Cisco Prime Collaboration Deployment:

- Cisco UC Virtualization Foundation (appears as "Foundation Edition" in vSphere Client)
- Cisco UC Virtualization Hypervisor Plus 6.0 or higher
- VMware vSphere Standard Edition, Enterprise Edition, or Enterprise Plus Edition
- Evaluation mode license (for example, for lab deployments and not production use)

The following are not compatible with Cisco Prime Collaboration Deployment:

- Cisco UC Virtualization Hypervisor (appears as "Hypervisor Edition" in vSphere Client)
- VMware vSphere Hypervisor Edition

Frequently Asked Questions About the Installation

Review this section carefully before you begin the installation.

How much time does the installation require?

The entire Cisco Prime Collaboration Deployment installation process, excluding pre- and postinstallation tasks, takes approximately 30 minutes.

What usernames and passwords do I need to specify?

Note The system checks your passwords for strength. For guidelines on creating a strong passwords, see "What Is a Strong Password?" below.

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

- Administrator account username and password
- Security password

You use the Administrator account username and password to log in to the following areas:

- Cisco Prime Collaboration Deployment GUI interface
- Command line interface

When you choose an administrator account username and password, follow these guidelines:

- Administrator account username—Must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator account password—Must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the administrator account password or add a new administrator account by using the command line interface. For more information, see the "Command line interface for Cisco Prime Collaboration Deployment" section.

For the security password, the password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

What is a strong password?

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

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

Avoid the following types of passwords:

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

Note Ensure that the ESXi and cluster passwords (install/discovered/migration) are less than 16 characters.

Can I install other software on the virtual machine?

You cannot install or use unapproved third-party software applications. The system can upload and process only software that is Cisco approved.

You can use the CLI to perform approved software installations and upgrades.

Preinstallation Tasks

The following table contains a list of preinstallation tasks that you must perform to install Cisco Prime Collaboration Deployment.

Table 2: Preinstallation Tasks

	Task
Step 1	Read this entire chapter to familiarize yourself with the installation procedure.
Step 2	Verify that the server on which you plan to install Cisco Prime Collaboration Deployment is properly configured in the DNS.
Step 3	Record the configuration settings for the server that you plan to install.

Allow Network Traffic

This section describes the minimum required ports that you must configure to support the Cisco Prime Collaboration Deployment server. The following table provides a summary of the ports that you must configure on a corporate firewall. The port configurations that are listed in this table are based on default settings. If you change the default settings, you must update these configurations.

If other servers or ports are required on your network, you must allow for that traffic.

Note Cisco Prime Collaboration Deployment migration requires the use of network file system (NFS) mounts on the ESXi host of the destination virtual machine. You may require additional protocols or ports. See the ESXi documentation at http://www.VMware.com for details.

Table 3: Corporate Firewall Configuration

Direction	Source	Destination	Protocol	Port	Description
Inbound	Cisco Prime Collaboration Deployment	IP address of the ftp server	TCP	21	FTP access to Cisco Prime Collaboration Deployment server for uploading licenses and software, upgrade, and CLI access
Inbound	Cisco Prime Collaboration Deployment	IP address of the sftp server	TCP	22	SFTP access to Cisco Prime Collaboration Deployment server for uploading licenses and software, upgrade, and CLI access

Direction	Source	Destination	Protocol	Port	Description
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTP	80	HTTP access to nonsecured GUI and web APIs (for example, login page)
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	111	Network File System
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTPS	443	HTTPS access to secured GUI and web APIs
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	662	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	892	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	2049	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	HTTPS	6060	Asynchronous SOAP messages from application servers
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTPS	8443	HTTP alternate

Direction	Source	Destination	Protocol	Port	Description
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTP	8080	HTTP alternate
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	UDP	32769	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP	32803	Network File System

Table 4: Use of Command Line Interface (CLI)/Cisco Platform Administrative Web Services (PAWS) for tasks

Infrastructure Requirements	Cluster Discovery	Migration	Upgrade Install COP Files	Restart	Switch Version	Fresh Install Edit/Expand	Readdress Task
VMware APIs	No	Yes	No	No	No	Yes	No
NFS mount on destination ESXi host of virtual machine	No	Yes (ISO install images)	No	No	No	Yes (ISO install images)	No
Local or remote SFTP	No	Yes (data export/import only)	Yes (ISO upgrade images)	No	No	No	No
PAWS	Yes when orchestrating UCM 10.0+ No when orchestrating UCM 6.1.5-9.1 (CLI used instead).		Yes	Yes	Yes	No	Yes
CLI via SSH	Yes	Yes	No	No	No	No	No

Gather Information for Installation

Use the following table to record information about Cisco Prime Collaboration Deployment. You may not need to obtain all the information; gather only the information that is relevant to your system and network configuration.

Note Because some of the fields are optional, they may not apply to your configuration.

Caution You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a field after installation; if so, the applicable CLI command is shown.

Table 5: Server Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID	This field specifies the Administrator account user ID that you use for secure shell access to the CLI on Cisco Prime Collaboration Deployment.	No, you cannot change the entry after installation. **Note** After installation, you can create additional Administrator accounts, but you cannot change the original Administrator account user ID.
Administrator Password	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI. You also use this password with the adminsftp user. You use the adminsftp user to access local backup files, upload server licenses, and so on. Ensure the password is at least six characters long; the password can contain alphanumeric characters, hyphens, and underscores.	Yes, you can change the entry after installation by running the following CLI command: **set password user admin**
Country	From the list, choose the applicable country for your installation.	Yes, you can change the entry after installation by running the following CLI command: **set web-security**

Parameter	Description	Can Entry Be Changed After Installation?
DHCP	Cisco requires that you choose **No** to the DHCP option. After you choose **No**, enter a hostname, IP address, IP mask, and gateway.	No, do not change the entry after installation.
DNS Enable	A DNS server resolves a hostname into an IP address or an IP address into a hostname. Cisco Prime Collaboration Deployment requires that you use a DNS server. Choose **Yes** to enable DNS.	No, do not change the entry after installation.
DNS Primary	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd.	Yes, you can change the entry after installation by running the following CLI command: **set network dns** To view DNS and network information, run the following CLI command: **show network eth0 detail**
DNS Secondary (optional)	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by running the following CLI command: **set network dns**
Gateway Address	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Without a gateway, you may limited to communicating only with devices on your subnet.	Yes, you can change the entry after installation by running the following CLI command: **set network gateway**

Parameter	Description	Can Entry Be Changed After Installation?
Hostname	Enter a hostname that is unique to your server. The hostname can consist of up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen. **Important** Do not change your hostname while any tasks are running.	Yes, you can change the entry after installation. **set network hostname**
IP Address	Enter the IP address of your server.	Yes, you can change the entry after installation. **set network ip eth0**
IP Mask	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: **set network ip eth0**
Location	Enter the location of the server. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: **set web-security**
MTU Size	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. The default value is 1500 bytes.	Yes, you can change the entry after installation by running the following CLI command: **set network mtu**

Parameter	Description	Can Entry Be Changed After Installation?
NTP Server	Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Caution** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node can be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.	Yes, you can change the entry after installation by running the following CLI command: **utils ntp server**
Organization	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry.	Yes, you can change the entry after installation by running the following CLI command: **set web-security**
Security Password	Enter your security password. The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password.	Yes, you can change the entry after installation by running the following CLI command: **set password user security**
State	Enter the state in which the server is located.	Yes, you can change the entry after installation by running the following CLI command: **set web-security**

Parameter	Description	Can Entry Be Changed After Installation?
Time Zone	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by running the following CLI command: **set timezone** To view the current time zone configuration, run the following CLI command: **show timezone config**

Begin Installation

You install the operating system and Cisco Prime Collaboration Deployment by running one installation program.

For information about how to navigate within the Installation wizard, see the following table.

Table 6: Installation Wizard Navigation

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

Install Cisco Prime Collaboration Deployment

Extract the PCD_VAPP.OVA File

Cisco Prime Collaboration Deployment is delivered with Unified Communications Manager, through a new purchase or an entitled upgrade that you access through the Product Upgrade Tool (PUT).

If you specify physical delivery in PUT, you will receive a DVD that contains an ISO file. You run this file to get an OVA file, which contains a preinstalled Cisco Prime Collaboration Deployment inside a virtual machine.

If you specify eDelivery in PUT, you will receive a Cisco Prime Collaboration Deployment download link in the email that contains media and license links. This link points to an OVA file that contains a preinstalled Cisco Prime Collaboration Deployment inside a virtual machine.

Procedure

Step 1 Extract the PCD_VAPP.OVA from the pcd_vApp_UCOS_10.xxxxx.iso file.
A new PCD_VAPP.OVA file is created. Verify the file size; ISO and OVA files do not have the same file size.

Step 2 Deploy the PCD_VAPP.OVA file in vCenter to install Cisco Prime Collaboration Deployment.
If you are using the vSphere client, the name of this file may be PCD_VAPP.OVA. If you are using the VMware vSphere web client to deploy the file, you must first change the name to PCD_VAPP.ova (lowercase) before you deploy the file.

Install the Virtual Machine

Before You Begin

- Download the OVA image.
- Read the “Preinstallation Tasks” section.
- Place a copy of the OVA on your local drive, depending on the installation type you are using.

Installation Type	Filename	Used with ESXi Host Software Version
OVA	PCD_VAPP.OVA or PCD_VAPP.ova **Note** The name of the OVA file depends on whether you are using vSphere client or VMware vSphere web client to deploy the file. For more information, see Extract the PCD_VAPP.OVA File, on page 14	4.1, 5.0, 5.5, and 6.0

- Determine the following information for creating a virtual machine for Cisco Prime Collaboration Deployment and mapping the required port groups:
  - A name for the new Cisco Prime Collaboration Deployment that is unique within the inventory folder and up to 80 characters.
  - The name of the host where the Cisco Prime Collaboration Deployment will be installed in the inventory folder.

- The name of the datastore in which the VM files will be stored.
- The names of the network port groups used for the VM.

Procedure

Step 1 Log in to vCenter.

Step 2 From the vSphere Client, choose **File** > **Deploy OVF Template**.

Step 3 Specify the location of the OVA file and click **Next**.
The **OVF Template Details** window opens and the product information is displayed, including the size of the file and the size of the VM disk.

Step 4 Click **Next**.

Step 5 Enter the name of your VM and select the location where the OVA will be deployed. Click **Next**.

Step 6 Select the data center or cluster on which to install the OVA. Click **Next**.

Step 7 Select the VM Storage Profile. Click **Next**.

Step 8 Select the Disk Format. Click **Next**.

Step 9 If necessary, select the network that the OVA will use for deployment. Click **Next**.

Step 10 Review the options that you selected, and if no changes are required, click **Finish** to begin the OVA installation.
After the installation is complete, the newly installed virtual machine appears in the selected location within vCenter.

Configure Cisco Prime Collaboration Deployment on the Virtual Machine

Cisco Prime Collaboration Deployment is installed as part of the OVA installation, but then you must configure it.

Procedure

Step 1 From the **vCenter** window, open the console of your newly installed virtual machine.

Step 2 Power on the virtual machine.
The installation begins automatically.

Step 3 When you are asked if you have preexisting configuration information, click **Continue** to proceed.

The **Platform Installation Wizard** screen appears.

Step 4 Click **Proceed** to continue with the wizard.

Step 5 Click **Continue** at the Basic Install screen.

Step 6 In the Timezone Configuration screen, select your time zone and click **OK**.

Step 7 Click **Continue** at the Auto Negotiation Configuration screen.

Step 8 When asked if you want to change the MTU size from the OS default, click **No** to proceed.

Step 9 For network configuration, you can choose to either set up a static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.

- If you have a DHCP server that is configured in your network and want to use DHCP, click **Yes**. The network restarts, and the Administrator Login Configuration window appears.
- If you want to configure a static IP address for the node, click **No**. The **Static Network Configuration** window appears.

Step 10 If you chose not to use DHCP, enter your static network configuration values and click **OK**.
The DNS Client Configuration window appears.

Step 11 To enable DNS, click**Yes**, enter your DNS client information, and click **OK**.
The network restarts by using the new configuration information, and the **Administrator Login Configuration** window appears.

Step 12 Enter your Administrator username and password.

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

Step 13 Enter the Certificate Information:

- Organization
- Unit
- Location
- State
- Country

Step 14 Click **OK** to proceed.

Step 15 Enter your Network Time Protocol (NTP) client configuration information. To test this configuration, click **Test**.

Step 16 Click **Proceed** to configure the NTP.

Step 17 When asked, enter your security password.

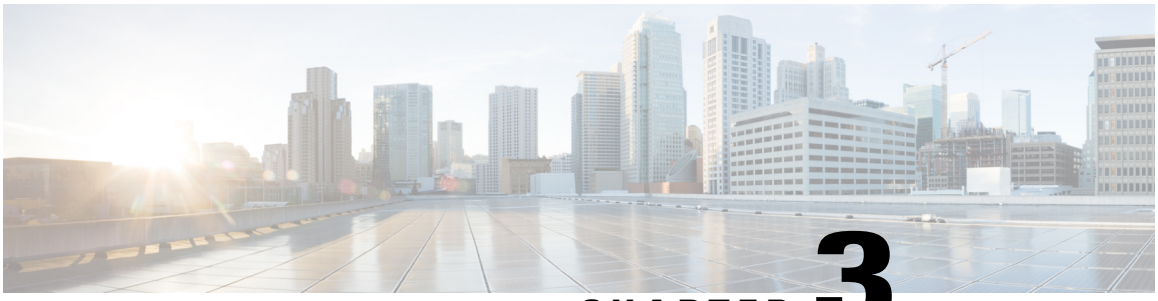
Step 18 When the platform configuration is complete, click **OK** to complete the installation. The installation take a few minutes to complete.

Postinstallation Tasks

Procedure

Step 1 Configure the backup settings. Remember to back up your Cisco Prime Collaboration Deployment data frequently. For details about how to set up a backup schedule, see CLI Commands and Disaster Recovery System, on page 135.

Step 2 Verify that you have a valid Network Time Protocol (NTP). To perform this check, log in to the Cisco Prime Collaboration Deployment CLI and run the command **utils ntp status**.



CHAPTER 3

Upgrade Cisco Prime Collaboration Deployment

- Upgrade Cisco Prime Collaboration Deployment Using CLI, page 19

Upgrade Cisco Prime Collaboration Deployment Using CLI

To upgrade the software version of Cisco Prime Collaboration Deployment, use the **utils system upgrade initiate** CLI command. There are four options, depending on where you have placed the new ISO file on an external filesystem or on Cisco Prime Collaboration Deployment itself.

Before You Begin

You must place the non-bootable ISO file on a network location or remote drive that is accessible from Cisco Prime Collaboration Deployment.

Procedure

Step 1 If you want to place the ISO on Cisco Prime Collaboration Deployment, upload it to the Cisco Prime Collaboration Deployment server `/upgrade` folder by performing the following steps:

a) sftp adminsftp@<Cisco Prime Collaboration Deployment IP>
b) cd upgrade
c) put <name of iso file>

Note If you are using a remote file system, place the ISO file there. Be sure that it can be accessed through SFTP or FTP.

Step 2 Log on to the CLI interface of the Cisco Prime Collaboration Deployment server, and use the **utils system upgrade initiate** CLI command.
You will be asked to choose an option, based on where your ISO is located.

```
Warning: Do not close this window without first canceling the upgrade.

1) Remote Filesystem via SFTP
2) Remote Filesystem via FTP
3) Local DVD/CD
4) Local Upload Directory
q) quit
```

```
Please select an option (1-4 or "q" ):
```

Step 3 Perform one of the following steps:

- If the ISO file is in the `/upgrade` folder of Cisco Prime Collaboration Deployment, choose option **4**.
- If the ISO file is on a remote file system, choose option **1** or **2**, depending on whether you wish to use SFTP or FTP.

Step 4 The system searches the directory for files to upgrade to and displays those filenames. Select the file that you wish to upgrade the Cisco Prime Collaboration Deployment system to by choosing the number of that file.

Step 5 Indicate whether you want the system to automatically switch to the upgraded version if the upgrade is successful.

Example:

```
Automatically switch
    versions if the upgrade is successful (yes/no): yes
```

Step 6 Start the installation:

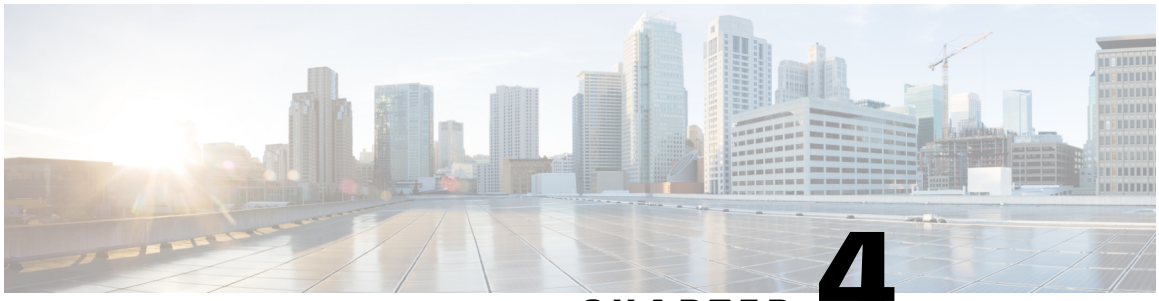
```
Start installation (yes/no): yes
The upgrade log is install_log_2013-10-07.20.57.17.log
Upgrading the system. Please wait...
10/07/2013 20:57:18 file_list.sh|Starting file_list.sh|<LVL::Info>
10/07/2013 20:57:18 file_list.sh|Parse argument
method=local_upload_dir|<LVL::Debug>
10/07/2013 20:57:18 file_list.sh|Parse argument source_dir=|<LVL::Debug>
10/07/2013 20:57:18 file_list.sh|Parse argument
dest_file=/var/log/install/downloaded_versions|<LVL::Debug>
```

The installation begins.

Step 7 After the installation is complete, use the **show version active** CLI command to see the current version of your Cisco Prime Collaboration Deployment software.

Example:

```
Active Master Version: 11.0.x.xxxxx-xxxx
Active Version Installed Software Options:
No Installed Software Options Found.
```



CHAPTER 4

Cisco Prime Collaboration Deployment Features

- Cisco Prime Collaboration Deployment Considerations, page 21
- Network Address Translation Support, page 23
- Supported Tasks for Applications and Versions, page 24
- Upgrade Paths for Export Restricted and Unrestricted Software, page 28
- Supported ESXi Server Versions, page 28
- Cluster Inventory, page 29
- Task Management, page 35
- Administration Tools, page 65
- FIPS 140-2 Compliance, page 74
- EnhancedSecurityMode Support, page 74
- Re-encryption through AES, page 76
- Limited Number of Sign-in Sessions, page 77

Cisco Prime Collaboration Deployment Considerations

Cisco Prime Collaboration Deployment allows a user to perform tasks (such as migration or upgrade) on servers that are in the inventory.

Step	Tasks
Step 1: Inventory Creation	To perform any tasks, you must first have clusters in your inventory. To add a UC cluster that is already running UC applications to your inventory, click the open and close navigation button and choose the **Inventory** > **Clusters** > **Discovery Cluster** feature. To migrate an existing cluster to new virtual machines, click the open and close navigation button and choose **Inventory** > **Clusters** > **Define Migration Destination Cluster**. (See Migration Task, on page 36.) To install a new cluster, click the open and close navigation button and choose the **Inventory** > **Clusters** > **Define New UC Cluster** feature. (See Install Task, on page 57.) If you are migrating an existing cluster to a new virtual machine cluster, or installing a new cluster, you must first add the ESXi Hosts that contain those virtual machines to your inventory. To add an ESXi host, click the open and close navigation button and choose **Inventory** > **ESXi Hosts**. (See Add an ESXi Host Server, on page 32.)
Step 2: Create a Task	You can create a task to perform an operation on a cluster in your inventory. During task creation, options allow you to: • Choose the cluster **Note** This task depends on the type of cluster you require. For example, you may choose a discovered cluster or a migration cluster. • Determine when to run the task • Determine if the task should run independently or pause between steps To perform one of the following actions, select from these procedures: • To migrate from an existing cluster to a new cluster of VM machines, see Migration Task, on page 36. • To upgrade the Unified Communications Manager version of an existing cluster, see Upgrade Task, on page 47. • To switch the version of an existing cluster, see Switch Versions Task, on page 50. • To restart an existing cluster, see Server Restart Task, on page 53. • To change the hostname or IP address of one or more servers in an existing cluster, see Readdress Task, on page 55. • To create a new UC cluster from VM machines, see Install Task, on page 57.
Step 3: Monitor Tasks	After a task is created, you can use the Monitoring window to view or track any task. You can also use this page to cancel, pause, or resume tasks. To view the tasks you created, see Monitor Task Status, on page 63.

Step	Tasks
Step 4: Administrative Tasks	You can set up email notification. See Email Notification, on page 156.

Network Address Translation Support

Cisco Prime Collaboration Deployment supports Network Access Translation (NAT). You can use Cisco Prime Collaboration Deployment in the following scenarios:

- When Cisco Prime Collaboration Deployment is in a local network or private network and application nodes are behind the NAT.
- When Cisco Prime Collaboration Deployment is behind the NAT and application nodes are in a private network.

To support application nodes behind the NAT, Cisco Prime Collaboration Deployment tracks the private IP address and the NAT IP address. Use Cisco Prime Collaboration Deployment to specify the NAT IP address for deployment nodes and the application. Cisco Prime Collaboration Deployment uses the NAT IP address to communicate with the application node. However, when you configure a node using the `platformConfig.xml` file, the node uses its private address.

Configure Cisco Prime Collaboration Deployment Behind the NAT

When Cisco Prime Collaboration Deployment is behind the NAT and communicates with an application virtual machine or an ESXi host, the communication occurs using the NAT IP address.

Note When Cisco Prime Collaboration Deployment is behind the NAT and application nodes are in a private network, the application nodes communicate with the NAT IP address.

Use the **NAT Settings** window in the **Administration** menu to set the NAT IP address for Cisco Prime Collaboration Deployment. The NAT IP address that you enter on this window does not appear on any window on the GUI.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **NAT Settings**.
The **NAT Settings** window appears and is prepopulated with the hostname and the private IP address.

Step 2 Enter the NAT IP address in the **NAT IP** field.

Step 3 Click **Save**.
The NAT IP address is saved as an entry in a configuration file on Cisco Prime Collaboration Deployment. This entry is used when the application nodes try to contact Cisco Prime Collaboration Deployment, then the

application nodes read the configuration file to get the NAT IP address, and then try to communicate Cisco Prime Collaboration Deployment with that IP address.

Step 4 (Optional) Click **Reset**.
The NAT IP address is reset to the earlier saved NAT IP address.

Supported Tasks for Applications and Versions

You can use Cisco Prime Collaboration Deployment to perform various tasks for Unified Communications applications. The following tables list the tasks that Cisco Prime Collaboration Deployment supports for each application.

- Table 7: Supported Tasks for Cisco Unified Communications Manager (including Session Management Edition), on page 24
- Table 8: Supported Tasks for Cisco Unified Presence, on page 25
- Table 9: Supported Tasks for the IM and Presence Service, on page 26
- Table 10: Supported Tasks for Cisco Unified Contact Center Express, on page 26
- Table 11: Supported Tasks for Cisco Unity Connection, on page 27

Note The releases listed in the tables do not specify the Engineering Special (ES)/ Service Update (SU) versions. To identify supported ES/SU versions that you can upgrade or migrate to through Cisco Prime Collaboration Deployment, see the release notes of the corresponding product, such as IM and Presence, Cisco Unified Communications Manager, and Unity Connection.

Note Cisco Prime Collaboration Deployment supports the destination version 10.x and above for an upgrade or a migration. The application versions 10.x and above support virtualization. If the source version is 8.x or 9.x on virtual machine, the upgrade task can upgrade to 10.x and above. However, if the source version is 8.x or 9.x on MCS, the upgrade task is not supported.

A migrate cluster task can migrate to any of releases listed in the tables, irrespective of whether on MCS 7800 or virtual machine, to 10.x or higher version on a virtual machine.

Table 7: Supported Tasks for Cisco Unified Communications Manager (including Session Management Edition)

Task	Release
Cluster Discovery	6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1)

Task	Release
Migrate Cluster (Install Application and Import Data from Old System)	**From** 6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1) **To** 10.x or 11.x
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1) **To** 10.x or 11.x
Restart	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1)
Switch Version	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.x, 10.5(1), 10.5(2), 11.0(1), 11.5(1)
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.x, 11.0(1), 11.5(1)

Table 8: Supported Tasks for Cisco Unified Presence

Task	Release
Cluster Discovery	8.5(x), 8.6(x)
Migrate Cluster (Install Application and Import Data from Old System)	**From** 8.5(4), 8.6(3), 8.6(4), 8.6(5) **To** 10.x or 11.x
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 8.6(3), 8.6(4), 8.6(5) **To** 10.x or 11.x
Restart	8.6(3), 8.6(4), 8.6(5)

Task	Release
Switch Version	8.6(3), 8.6(4), 8.6(5)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	Not applicable
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	Not applicable

Table 9: Supported Tasks for the IM and Presence Service

Task	Release
Cluster Discovery	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1)
Migrate Cluster (Install Application and Import Data from Old System)	**From** 9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1) **To** 10.x or 11.x
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1) **To** 10.x or 11.x
Restart	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1)
Switch Version	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.x, 10.5(1), 10.5(2), 11.0(1), 11.5(1)
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	Not Supported

Table 10: Supported Tasks for Cisco Unified Contact Center Express

Task	Release
Cluster Discovery	8.5(1), 9.0, 9.0(2), and 10.x, 11.x
Migrate Cluster (Install Application and Import Data from Old System)	Not Supported

Task	Release
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 9.0(2), 10.x, 11.x **To** 10.x or 11.x
Restart	9.0(2), 10.x, 11.x
Switch Version	9.0(2), 10.x, 11.x
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.5(x), 11.x
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.5(x), 11.x

Table 11: Supported Tasks for Cisco Unity Connection

Task	Release
Cluster Discovery	8.6.1, 8.6.2, 9.x, 10.x, 11.x
Migrate Cluster (Install Application and Import Data from Old System)	Not Supported
Upgrade Cluster (Upgrade Application Version or Install COP Files)	From 8.6(x) to 8.6(x) From 8.6(x) to 9.x From 9.x to 9.x From 10.0(1) to 10.x From 10.x to 11.0 From 11.0 to 11.x
Restart	8.6(1), 8.6(2), 9.x, 10.x, 11.x
Switch Version	8.6(1), 8.6(2), 9.x, 10.x, 11.x
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.5(x), 11.x
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.5(x), 11.x

Upgrade Paths for Export Restricted and Unrestricted Software

The following table lists the supported upgrade paths for applications that have an export restricted and an export unrestricted version. You can identify which version of an application you have by looking at the license SKU: export unrestricted versions are indicated by XU and export restricted versions are indicated by K9.

Table 12: Supported Upgrade Paths for Export Restricted and Unrestricted Software

From	To	Task Types Supported
Export Restricted (K9)	Export Restricted (K9)	Supported for Upgrade paths Supported for Migration paths
Export Restricted (K9)	Export Unrestricted (XU)	Not supported for Upgrade paths Supported for Migration paths
Export Unrestricted (XU)	Export Restricted (K9)	Not supported for Upgrade paths Not supported for Migration paths
Export Unrestricted (XU)	Export Unrestricted (XU)	Supported for Upgrade paths Supported for Migration paths

Related Topics

Create an Upgrade Task, on page 47
Create a Switch Versions Task, on page 50

Supported ESXi Server Versions

Following table lists the supported ESXi server versions for a Cisco Prime Collaboration Deployment virtual machine (VM). This VM integrates through the VMware APIs with a virtualization host that is running VMs for Cisco Unified Communications Manager or other applications. To view the list of compatible versions of VMware vSphere ESXi server for a Cisco Prime Collaboration Deployment virtual machine that runs on a virtualization host, see http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

VMware vSphere ESXi on Host having VM of Cisco Unified Communications Manager or Another Application	Cisco Prime Collaboration Deployment Version Compatibility for VMware APIs
5.1 and older	No
5.5	Yes

VMware vSphere ESXi on Host having VM of Cisco Unified Communications Manager or Another Application	Cisco Prime Collaboration Deployment Version Compatibility for VMware APIs
6.0	• No—For Release 11.5(1) • Yes—For Release 11.5(1) SU1 and later

Cluster Inventory

You must add a cluster to the Cisco Prime Collaboration Deployment inventory before you can use it in a task. The Discover Cluster feature is used to add existing clusters to the inventory. To create a new cluster by migrating an old cluster to new virtual machines, click **Define Migration Destination Cluster**. To install a new cluster, click **Define New UC Cluster**.

Discover a Cluster

With the Discover Cluster feature, Cisco Prime Collaboration Deployment communicates with the servers that are already running Unified Communications applications and adds that cluster information into the Cisco Prime Collaboration Deployment inventory.

When you perform the Discover Cluster operation, the Cisco Prime Collaboration Deployment server communicates with the publisher of the cluster and retrieves the cluster information. Then, it communicates with each server, installs the `ciscocm.ucmap_platformconfig.cop` file on the server (to retrieve configuration information), and collects information about the hostname, IP, product type, and both active and inactive versions for that server.

Note When the publisher is behind the NAT, providing the private IP address of the publisher does not reach to the node. You must provide the proper IP address for successful node discovery.

For details on the supported applications, see “Supported Upgrade and Migration Tasks” in the Related Topics section.

Note If a cluster includes Cisco Unified Communications Manager and Cisco Unified Presence (Cisco Unified Communications and IM and Presence Service servers), the Cluster Discovery discovers the Cisco Unified Presence or IM and Presence Service nodes as part of the Cisco Unified Communications Manager cluster.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **Clusters**.

The **Clusters** window appears.

Step 2 Click the **Discover Cluster** button to discover the existing clusters.
The Discover Cluster wizard appears.

Step 3 Enter details in the following fields:

- **Choose a Nickname for this Cluster**
- **Hostname/IP Address of Cluster Publisher**
  Note For a cluster that has both Unified Communications Manager and IM and Presence Service nodes, enter the hostname or IP address of the Cisco Unified Communications Manager publisher.
- **OS Admin Username**
- **OS Admin Password**
- **Enable NAT**

Step 4 (Optional) Check the **Enable NAT** check box, and then click **Next**.
Important During discovery, the `ciscocm.ucmap_platformconfig.cop` file is installed automatically on the active partition of all nodes in the cluster. This COP file is used for the cluster discovery process and does not affect Cisco Unified Communications Manager.
Note When a cluster is behind NAT, the application tries to establish communication with each node using its private address. So, the nodes are unreachable. A pop-up shows the unreachable nodes.
Cisco Prime Collaboration Deployment generates a list of cluster nodes from the inventory of the publisher server. The list generation process may take several minutes to complete. After the list is generated, a confirmation message appears indicating the completion of the cluster discovery process.

Step 5 Click **Edit** to add NAT IP address, and click **OK**.
The Nat IP address is set for the hostname.

Step 6 Click **Resume Discovery** to resume the discovery of unreachable nodes.
Cisco Prime Collaboration Deployment retries to discover the cluster with the NAT IP address instead of the private IP address and to get the cluster details, such as version. The discovery is successful when the cluster details appear on the window.

Step 7 Click **Next**.

Step 8 (Optional) Click **Assign Functions** to assign functions to each of the cluster nodes.
Note The assignment of functions has no effect on the services that are to be activated. However, this information can be used to determine the default sequence of tasks.
The **Assign Functions** dialog box appears.

Step 9 Click **Finish**.
The cluster appears in the **Clusters** window, showing the cluster name, the product and version, the cluster type as `Discovered`, and the discovery status.
Note It might take a few minutes to discover a cluster. After the discovery is complete, the information for each node in the cluster is listed in the **Cluster Inventory** window. If you cancel the discovery before it is complete, the data is lost and you will have to repeat the discovery procedure.

Note The following are the different statuses that appear for the **Discovery Status** field:

- **Contacting—**Indicates that Cisco Prime Collaboration Deployment is establishing communication with clusters.
- **Discovering—**Indicates that the cluster discovery is in process.
- **Successful—**Indicates that the cluster discovery is successful.
- **Node Unreachable—**Indicates that the cluster node is inaccessible.
- **Timeout—**Indicates that the duration that is configured for the cluster discovery is complete but no cluster was discovered.
- **Internal Error—**Indicates that cluster discovery is failed because of an incorrect NAT IP address.

Related Topics

Supported Tasks for Applications and Versions, on page 24
Upgrade Paths for Export Restricted and Unrestricted Software, on page 28

Modify and View a Cluster

You can select one or multiple virtual machines that you have added as nodes in a cluster to view and modify them.

Note The cluster nodes that you need to install appear as editable and have **Edit** and **Delete** links. The installed cluster nodes appear dimmed and you cannot edit or delete them.

Note When you add new nodes to the installed cluster, all fields on **Configure NTP Settings** page appear dimmed and are non-editable. The fields on the other pages will populate the values of the already installed nodes as the default. If needed, you can change the values for the newly added nodes.

Procedure

Step 1 Discover a cluster by following the Discover a Cluster procedure. See Discover a Cluster, on page 29.

Step 2 Check the check box of one of the discovered or newly installed clusters to choose a cluster, and click the **Edit** link.

Step 3 On the **Edit Link** window, view the details in the fields, and modify the details, as required.

Step 4 Click **OK**.

Add an ESXi Host Server

Important When you add an ESXi host into Cisco Prime Collaboration Deployment, you mount the Cisco Prime Collaboration Deployment server as a network file system (NFS) mount on that host. In future, if you remove your Cisco Prime Collaboration Deployment machine, you should first delete the ESXi host from the Cisco Prime Collaboration Deployment so that it does not cause a stale NFS mount on that host.

To communicate with an ESXi host server, Cisco Prime Collaboration Deployment requires either root access to the ESXi software or a nonroot user with **Host** and **Virtual Machine** privileges enabled. The administrator creates a nonroot user with the specific permissions for Cisco Prime Collaboration Deployment tasks, such as power on and off and mounting ISO or floppy, for fresh install or migration. The length of the nonroot user password must be less than 16 characters.

Note When you shut down a Cisco Prime Collaboration Deployment server, we recommend that you use the **utils system shutdown** CLI command.

Note Make sure that the host with the Cisco Prime Collaboration Deployment VM and the host with the application VMs use the required Virtualization Software License. See Virtualization Software License Types, on page 4.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **ESXi Hosts** from the menu.

Step 2 Click **Add ESXi Host**.

Step 3 The **Add Host Server** dialog box appears. Enter the following information:

a) Hostname/IP Address
b) Root sign-in or sufficiently privileged nonroot sign-in
c) Root password or nonroot password

Step 4 Click **OK** to add the ESXi host.

Create a Migration Cluster

Before You Begin

To create a migration task, perform the following procedure:

1 Discover the existing cluster you wish to migrate. See the "Discover a Cluster" procedure at Discover a Cluster, on page 29.

2 Define a migration cluster.

Note After you define the migration cluster, see "Migration Task" at Migration Task, on page 36 to define when and how to perform the migration.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, select **Inventory** > **Cluster**.

Step 2 Click **Define Migration Destination Cluster**.
The **Define Migration Destination Cluster** wizard appears.

Step 3 In the Specify Clusters section, specify the name of the cluster, select the source UC cluster from the drop-down list. Enter a name in the Destination Cluster Name field and select one of the following Destination Network Settings options:

- To retain the default network options, select the **Use the source node network settings for all destination nodes** option.
- To modify the default network settings or enter new network options, select the **Enter new network settings for one or more destination nodes** option.

Note If you select the **Use the source node network settings for all destination nodes** option, same IP address appears for both the source node **NAT IP** and **Dest NAT IP** columns **Assign Destination Cluster Nodes**. If you select the **Enter new network settings for one or more destination nodes** option, only source hostname appears and not the destination hostname on the **Assign Destination Cluster Nodes** window.

Step 4 Click **Next**.
The **Assign Destination Cluster Nodes** window appears.

Step 5 Click the **Assign Destination Cluster Nodes** button to select the destination virtual machine for each source node.

Note If DHCP is in use on your source node, the destination node will also be configured to use DHCP, and you will not have the option of changing your network settings in this wizard.

The **Configure Destination Cluster** window appears.

Step 6 Select a virtual machine, click **Next Node** to go to the next node in the cluster, and select another virtual machine for the destination virtual machine, and click **Done**.

Note If there is more than one node in the cluster, repeat these steps - (assigning VM, and entering new IP/hostname settings, if needed) for each node in the source cluster.

Step 7 Click **Next**.
The **Configure NTP/SMTP Settings** window appears.

Step 8 Enter the Network Time Protocol (NTP) server settings to be applied to the migration nodes when the migration task runs, and optionally, enter the SMTP server settings.

Important In a proxy TFTP setup, if a network migration is performed "off-cluster", you need to manually configure the new hostname and IP address of that off-cluster in the proxy TFTP. Off-cluster refers to situations where TFTP functionality is being performed by a proxy that is not part of that specific Unified Communications Manager cluster. During a migration, that TFTP server (that is not part of the cluster) is not modified. If you want to change the hostname or IP address of that server, you must do it as a separate process and not with Cisco Prime Collaboration Deployment.

Step 9 Click **Next**.
The **Define DNS Settings** window appears.

Step 10 To change the DNS setting for a node, select the node or nodes from the table and click **Assign DNS Settings**. Enter the primary and secondary DNS, then click **OK** to apply the changes.

Important You cannot change the domain name during a migration.

Step 11 Click **Finish**.
The changes are saved and a row is added to the clusters table to reflect the new migration cluster that you have created.

Add New Cluster for Fresh Install

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, select **Inventory** > **Clusters**.

Step 2 Click **Define New UC Cluster**.
The **Define Cluster** wizard appears.

Step 3 In the Specify Cluster Name section, enter the cluster name, and click **Next**.
The **Add Virtual Machines** window appears.

Step 4 Click **Add Node** to add nodes to the cluster.
The **Add Node** dialog box appears showing the list of the available VMs that are sorted by name and by host.

Step 5 On the **Add Node** window, enter the network settings for the node that you have added, choose the functions for the node, and choose a VM for this node. Select the VM that you wish to add and then enter the following information in the sections below the VM table:

a) In Network section, select either **Static IP Address** or **Use DHCP with reservations**. If you select the **Static IP Address** option, enter the hostname, IP Address, subnet mask, gateway, and NAT IP. If you select **Use DHCP with reservations** option, enter the IP address that you have a reservation for on your DHCP server (associated with the MAC address for that VM) in addition to the hostname.
If you are adding a Cisco Unified Contact Center Express server, do not use DHCP for network settings.

Note **NAT IP** is an optional field. In Step 4, if you have selected a node that is behind NAT, enter the IP address in the **NAT IP** field, else leave this field blank. The value that you enter in this field appears in the **NAT IP** column. If the NAT IP address is associated with a port, you can enter port value which should be in the range of 1 to 65535.

b) From the **Products and Functions** list box, select a product.

c) In the Functions section, check the appropriate function check boxes for your VM.

Note
- Check the **Publisher** check box for at least one node in the cluster that you have defined, for each application type.
- (Optional) Add a note about the functions that you have assigned in the **Notes** field below the **Publisher** field.

d) Click **OK**.

e) In Virtual Machines section, choose a VM for this node.

Note
- Choose a new VM for fresh install clusters and that new VMs must be in turned off state.
- Do not install over an existing running Cisco Unified Communications Manager node. The installation must be a fresh VM that you create with the appropriate OVA for the application that you will install.

Step 6 Click **OK**.
The VM is added and is listed in the **Cluster Name** table.

Step 7 (Optional) To add more nodes to the cluster, repeat steps 4 through 6.

Step 8 Click **Next**.
The **Configure Cluster Wide Settings** window appears.

Step 9 Enter the OS administration credentials, application credentials, security password, SMTP settings, and certificate information for this cluster, and click **Next**.
The **Configure DNS Settings** window appears.

Step 10 (Optional) Add a DNS setting for a node, select the node, and click **Assign DNS Settings**.
The Cisco Unified Contact Center Express application must use DNS.
The **Configure NTP Settings** window appears.

Step 11 Enter IP address of at least one NTP server.

Note
- It is recommended that you define at least IP addresses of two NTP servers.
- If you are not using DNS, NTP server must be an IP address. If you are using DNS, NTP server can be an FQDN.

Step 12 Click **Next**.
The **Configure NIC Settings** window appears.

Step 13 (Optional) Choose the server, and enter an MTU size between 552 and 1500, and click **Apply to Selected**.

Step 14 Click **Next**.
The **Configure Time Zones** window appears.

Step 15 Select a node, choose the region and time zone from the **Region** and **Time Zones** list boxes, and click **Apply to Selected**.

Step 16 Click **Finish**.
The new install cluster is listed on the Clusters screen, with a Cluster Type as **New Install**. The cluster is defined but is yet to be created. To install the cluster, create an install task. The install task uses the install cluster you have defined, and creates the cluster.

Task Management

After you add your clusters and ESXi hosts to the Cisco Prime Collaboration Development inventory, you can create tasks to manage your clusters. Each task has the following common features:

- Each task is applied to a single cluster.
- The default sequence for each task (for example, what servers are affected and when) is applied based on the server functions you defined.
- The sequence of each task can be customized to fit your needs.
- Each task can be scheduled to start immediately or at a later date.

- Tasks can also be created without a specific start time. You can then manually start the task through the Monitoring page at the appropriate time.

Migration, install, and upgrade tasks require you to select one or more Cisco Option Packages (COP) or ISO files. You must download these files from Cisco.com and upload them to the Cisco Prime Collaboration Deployment server before you create the task. You can use any SFTP client to upload the files using the "adminsftp" account and the OS Administation password. Upload migration and .iso install files into the `/fresh_install` directory, and place upgrade .iso files or .cop files to be installed on an existing server in the `/upgrade` directory.

Note Migration and install .iso files must be bootable.

Migration Task

Before You Begin

To perform cluster migration, the destination virtual machine must be ready for installation before you create the migration task. Be sure that the following steps are completed:

1. **VMware—**Deploy the hardware for the new cluster and install ESXi.

Note Make sure that the host with the Cisco Prime Collaboration Deployment VM and the host with the application VMs use the required Virtualization Software License. See Virtualization Software License Types, on page 4.

2. **ISO file—**Download the recommended OVA and ISO images for the target release, and use SFTP to send the ISO file to the Cisco Prime Collaboration Deployment server, `/fresh_install` directory.
3. **VMware—**Deploy the Cisco-recommended OVA to create the VMs for the destination nodes. Create the appropriate number of target virtual machines on your ESXi hosts (one new virtual machine for each server in the existing cluster) using the Cisco OVAs that you downloaded in Step 2. Configure the network settings on new VMs.
4. **Cisco Prime Collaboration Deployment GUI—**Add the ESXi Hosts that contain your virtual machines to the Cisco Prime Collaboration Deployment inventory. For information about adding an ESXi host to Cisco Prime Collaboration Deployment, see Add an ESXi Host Server, on page 32.
5. **Cisco Prime Collaboration Deployment GUI—**Ensure that you performed a cluster discovery for the existing cluster (source cluster) so that it appears in the Cluster Inventory. For information about cluster discovery, see Discover a Cluster, on page 29.
6. **Cisco Prime Collaboration Deployment GUI—**Create the migration cluster (click the open and close navigation button and choose **Inventory** > **Clusters**) to define the mapping between MCS source nodes and target virtual machines.

Important When the migration cluster is created, you must indicate whether all destination nodes will maintain the same hostname or IP address, or whether some of these addresses will change.

- Using the source node settings for all destination nodes option is called a simple migration. See the migration flow chart for more information.
- Entering new network settings for one or more destination nodes is called a network migration. See the migration flow chart for more information.

7 **Cisco Prime Collaboration Deployment GUI—**Setup Email Notification (Optional)

- Click the open and close navigation button and choose **Administration** > **Email Notification**.
- When email notification is set up, the Cisco Prime Collaboration Deployment server emails the error conditions that may occur during the migration task.

8 **Cisco Prime Collaboration Deployment GUI—**Create the migration task.

9 Install the `ciscocm.migrate_export_10_0_1.sh_v1.1.cop.sgn` cop file on both IM and Presence publisher and subscriber nodes.

Special Considerations

- If you are migrating a cluster that is security enabled, see CTL Update, on page 149 for special instructions. If you are performing a migration with network migration (where one or more hostnames or IP addresses change between the source and destination nodes), update the IP addresses or hostnames of destination nodes in your DNS server before you begin the migration task.
- You can specify a different NAT address for source and destination, so that the source is not abruptly shut down. If you want to perform a simple migration but need to specify different Network Address Translation (NAT) entries for source and destination, you must select “Network Migration” and provide the same details for source and destination (all hostnames and IP addresses).

Create a Migration Task

Follow these steps to create or edit a new migration task to simultaneously upgrade and migrate a cluster to new virtual machines.

Note the supported restricted and unrestricted paths. See “Supported Upgrade and Migration Tasks” and “Upgrade Paths for Export Restricted and Unrestricted Software” in the Related Topics section.

Procedure

Step 1 Click the open and close navigation button and choose **Task** > **Migrate**.

Step 2 Click the **Add Migration Task**. The Add Migration Task wizard appears.

Step 3 From the **Source UC Cluster** drop-down list, select the cluster on which the nodes to be migrated from are located.

Step 4 From the **Destination Cluster** drop-down list, select the destination cluster or migration map. The migration maps are associated with the source cluster you have selected. Click **Next**.

Step 5 In the **Choose Migration Files** section, choose the ISO file you wish to install on the destination cluster by clicking **Browse**. The **Choose a Migration File** window opens. Select the ISO file from the list and click **OK**.

Important The ISO file is visible here only if it was placed in the directory under `/fresh_install`, uploaded through a standard SFTP client (Admin Name: adminsftp, Password: Administration password). For more information, see the task management information at the beginning of this section.

Step 6 Click **Next**.

Step 7 In the **Set Start Time** section, choose between scheduling a particular start time, starting the task immediately, or starting the task manually at some point in the future. Click **Next**.

Step 8 In the **Specify Migration Procedure** section, you will see the default sequence for the migration task. If you wish, you can change the sequence of steps in the migration procedure. (For example, the default is to install each subscriber individually. You might want to change this to install more than one subscriber in a step.) You have the following options:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step. If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be performed earlier.
Down arrow	Move the step down to be performed later.

- The Pencil icon opens up an **Edit Step** window. Add nodes to be migrated in this step from the list of available nodes. The available nodes are the ones that you chose for migration.
- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.
  Important You cannot proceed to the next step until you assign all the nodes.
- The **Pause task after step completes** option pauses the task after completion of this step. You must manually start the next step to complete the task.

For more information about sequencing tasks, see the task management information at the beginning of this section.

Step 9 Click **Next**.

Step 10 In the **Review** section, you can review the selections that you made. You can also add notes to your new migration task.

Step 11 If there are no changes required, click **Finish** to add your new migration task.

Step 12 The new migration task appears in the table on the Migrate screen.

Important If you are performing a migration with network migration, the sequence automatically inserts a "Forced Pause" step into the sequence after all the servers are installed to allow the user to perform procedures. See the "Run a Migration Task" section for details on when manual procedures are needed. The "Forced Pause" step cannot be edited and moved, and it has no nodes assigned. This step is inserted before the source node shutdown step, because if CTL Updates or certificate management steps are required, these steps must be completed before the source node is shut down.

Related Topics

Supported Tasks for Applications and Versions, on page 24
Upgrade Paths for Export Restricted and Unrestricted Software, on page 28

Run a Migration Task

If you scheduled the task to start at a later date, or if you chose Manual Start, then the task is listed in the task list, but has not started yet. In this case, a validation button will be associated with the task. Click **Validate** to check the task before it runs. If there are any problems with the task (such as a missing ISO file, or VMs not in Off state), the validation will alert you, so the issues can be fixed before the task starts.

For a task that was scheduled to start, you can click the Start button to begin the task.

While the migration task is running, depending on the type of migration task, some user operations might be needed. For example, if you are performing a "migration with network migration," the sequence automatically inserts a "Forced Pause" into the sequence after all the servers have been installed. This will cause the migration task to pause after all the new servers are installed but before any of the source machines are shut down.

Consult the table below and the applicable Migration Procedure flow chart (see the "Migration Procedure Flow Charts" section) to determine if any user interaction will be needed during the migration task.

Important When the migration cluster is created, you must indicate whether all destination nodes will keep the same hostname or IP address, or if some of these addresses will be changing.

- Using the source node settings for the all destination nodes option is referred to as a "simple migration" in the "Migration Procedure Flow Charts" section.
- Entering new network settings for one or more destination nodes option is referred as "network migration" in the "Migration Procedure Flow Charts" section.

Unified CM source cluster - from Release	Simple Migration or Network Migration	Unified CM source cluster - (secure or nonsecure)	User procedures to be performed during migration
6.1(5), 7.1(3), 7.1(5)	Simple migration	Secure	No steps are required during migration
6.1(5), 7.1(3), 7.1(5)	Simple migration	Nonsecure	No steps are required during migration
6.1(5), 7.1(3), 7.1(5)	Network migration	Secure	When migration task reaches the Forced Pause step, click the Resume button.

Unified CM source cluster - from Release	Simple Migration or Network Migration	Unified CM source cluster - (secure or nonsecure)	User procedures to be performed during migration
6.1(5), 7.1(3), 7.1(5)	Network migration	Nonsecure	When migration task reaches the Forced Pause step, click the Resume button.
8.x, 9.x, and 10.x	Simple migration	Secure	No steps required during migration
8.x, 9.x, and 10.x	Simple migration	Nonsecure	No steps required during migration
8.x, 9.x, and 10.x	Network migration	Secure	When the migration task reaches the Forced Paused step, perform the following steps: **1** CTL Update **2** Bulk Certificate Management **3** Resume the task on Cisco Prime Collaboration Deployment GUI.
8.x, 9.x, and 10.x	Network migration	Nonsecure	When the migration task reaches the Forced Paused step, perform the following steps: **1** Bulk Certificate Management **2** Resume the task on Cisco Prime Collaboration Deployment GUI.

Postmigration Tasks for Cisco Unified Communication Manager Nodes in the Cluster

“After the migration task runs successfully, if a migration task with network migration was performed, some additional steps are required. (No postmigration tasks are required if a simple migration was performed.) ” Consult the following table and the applicable migration Use Case flowchart to determine whether any user tasks must be performed after the migration task is successful.

Unified CM source cluster - from Release	Simple Migration or Network Migration	Unified CM source cluster (Secure or Non-secure)	User procedures to be performed after migration
6.1(5), 7.1(3), 7.1(5)	Network migration	Secure	**1** Perform CTL Update **2** Restart Services on Unified Communications Manager **3** Change TFTP Server IP Address **4** Verify Phone Registration
	Network migration	Nonsecure	**1** Change TFTP Server IP Address **2** Verify Phone Registration

Unified CM source cluster - from Release	Simple Migration or Network Migration	Unified CM source cluster (Secure or Non-secure)	User procedures to be performed after migration
8.x, 9.x, and 10.x	Network migration	Secure	1 Change TFTP Server IP Address 2 Verify Phone Registration
	Network migration	Nonsecure	1 Change TFTP Server IP Address 2 Verify Phone Registration

Post Migration Tasks for IM and Presence Service

If the migrated cluster contains IM and Presence Service nodes, and you are performing a network migration, these postinstallation tasks must be performed for any pre-Release 10.x IM and Presence Service cluster.

Procedure

	Command or Action	Purpose
Step 1	Configure certificates and certificate trust stores.	If the old cluster had CA-signed certificates in any of the component trust stores, be aware that the components contain self-signed certificates on the migrated Release 10.x cluster. Also, the root and intermediate certificates of the Certificate Authority are not preserved in their respective trust stores. You should sign the certificates with the old Certificate Authority, similar to how it would have been done initially. For more information, see the *Administration Guide for Cisco Unified Communications Manager Guide*.
Step 2	Configure intercluster peers.	If the old cluster had an intercluster peer relationship, you need to delete the configuration from all peer clusters. Once this is done, add the appropriate interclustering based on the network details of the new cluster. For example, Cluster A, Cluster B, and Cluster C are all intercluster peers. If Cluster A was migrated, then you should delete all interclustering configuration from the old Cluster A and likewise Cluster A from Cluster B and Cluster C and then add interclustering with the network details of the new Cluster A. You do not need to configure anything from the new Cluster A since the migration brings over the old data. For more information, see *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.*
Step 3	Re-publish SIP Federation.	If the old cluster was front-ending SIP Interdomain with Microsoft OCS/Lync/AOL or SIP Intradomain federation with OCS/Lync, then your enterprise will need to re-publish the DNS-SRV of your federating domain to reflect the new network details. If the far side has SIP static routes configured instead of DNS-SRV based routing, then the SIP static routes need to be changed to reflect the new network address. Similarly, all intermediate network elements (including ASA or any other similar components that route or inspect traffic to the old cluster from the external federation entities) need to be re-configured for successful routing to the new cluster. For Interdomain configuration, see

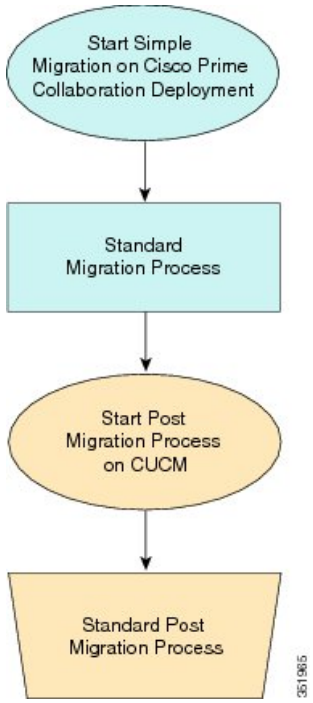
	Command or Action	Purpose
		Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager. For Intradomain federation, see *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.
Step 4	Re-publish XMPP Federation.	If the old cluster was front-ending XMPP Interdomain federation to any external XMPP servers, then your enterprise will need to republish your federating domain's DNS-SRV records to reflect the new network details. Refer to *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.
Step 5	Configure Cisco Jabber/Cisco Unified Personal Communicator connectivity.	Jabber or Unified Personal Communicator caches the hostname information from the old cluster and does not have new hostname information unless you are able to push the configuration to the desktop of the user, or that user manually enters one of the node names. A fail safe approach for users that are unassigned from the old cluster, and as a result are unable to log in, involves the user manually entering the hostname or IP address of one of the nodes in the new cluster (of which they were informed of prior to migration). In this scenario, the user's client finds the right home node by way of redirected login.

Migration Procedure Flow Charts

Use the following task flows as a guide to perform migration tasks.

Simple Migration

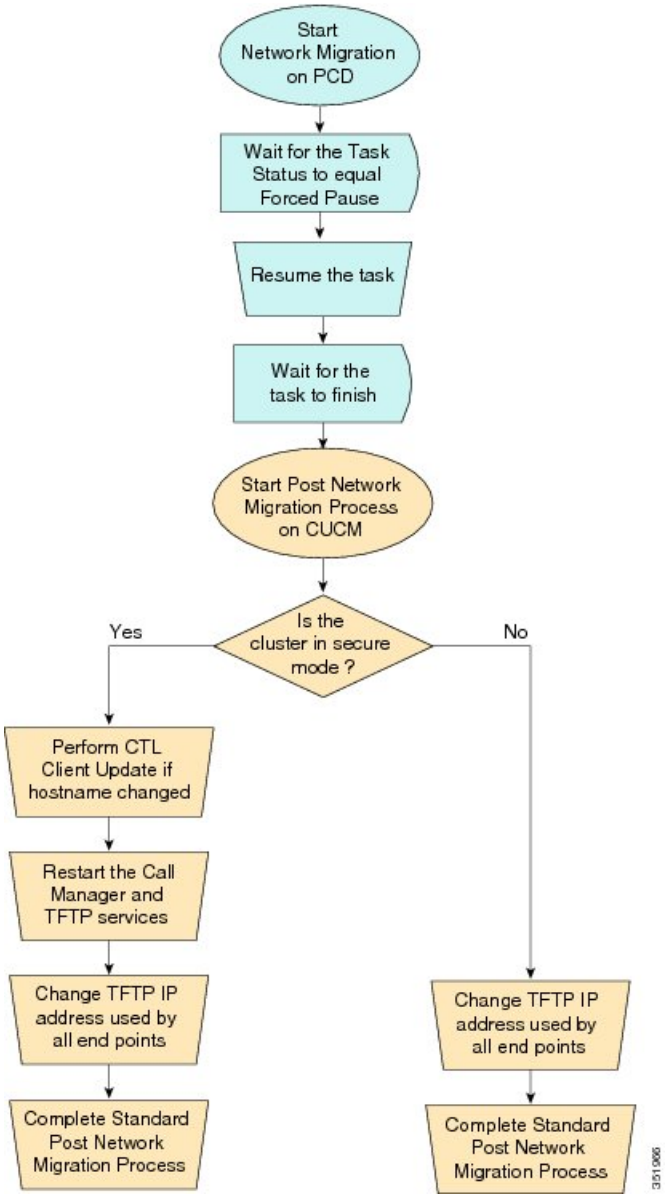
Figure 1: Flow Chart for Simple Migration



Note Cisco Prime Collaboration Deployment does not support migration of Business Edition 5000 Appliance running on MCS 7828H3.

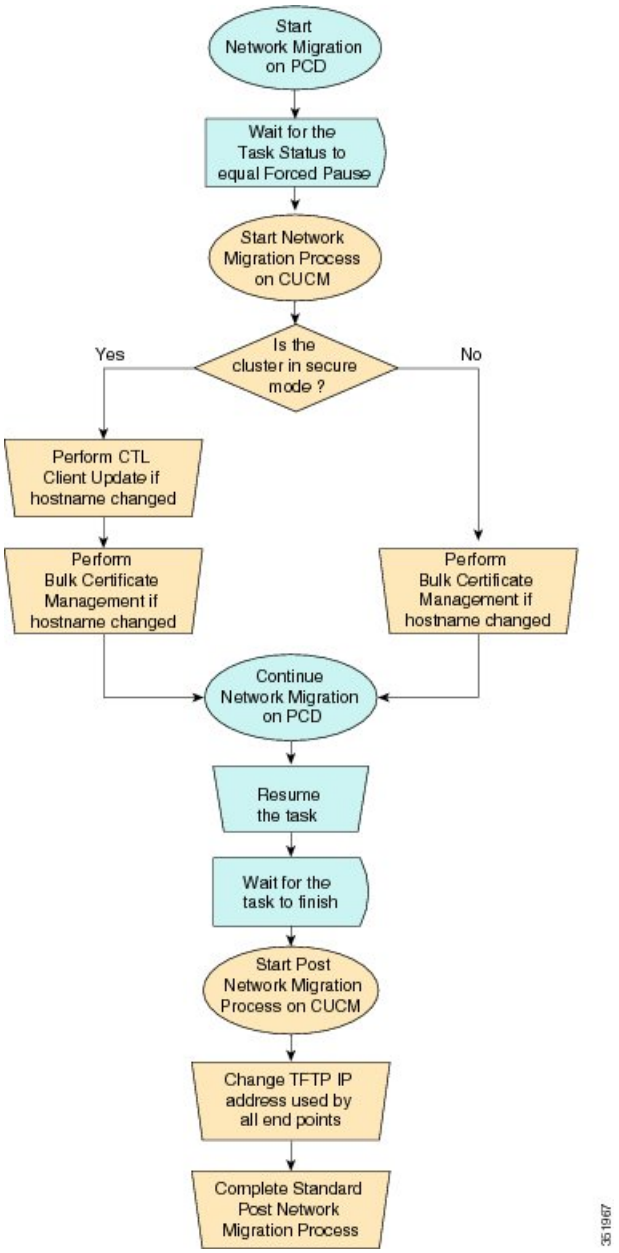
Pre Release 8.0.1 Unified CM Network Migration

Figure 2: Flow Chart for Pre Release 8.0.1 Unified Network Migration



Release 8.0.1 And Later Unified CM Network Migration

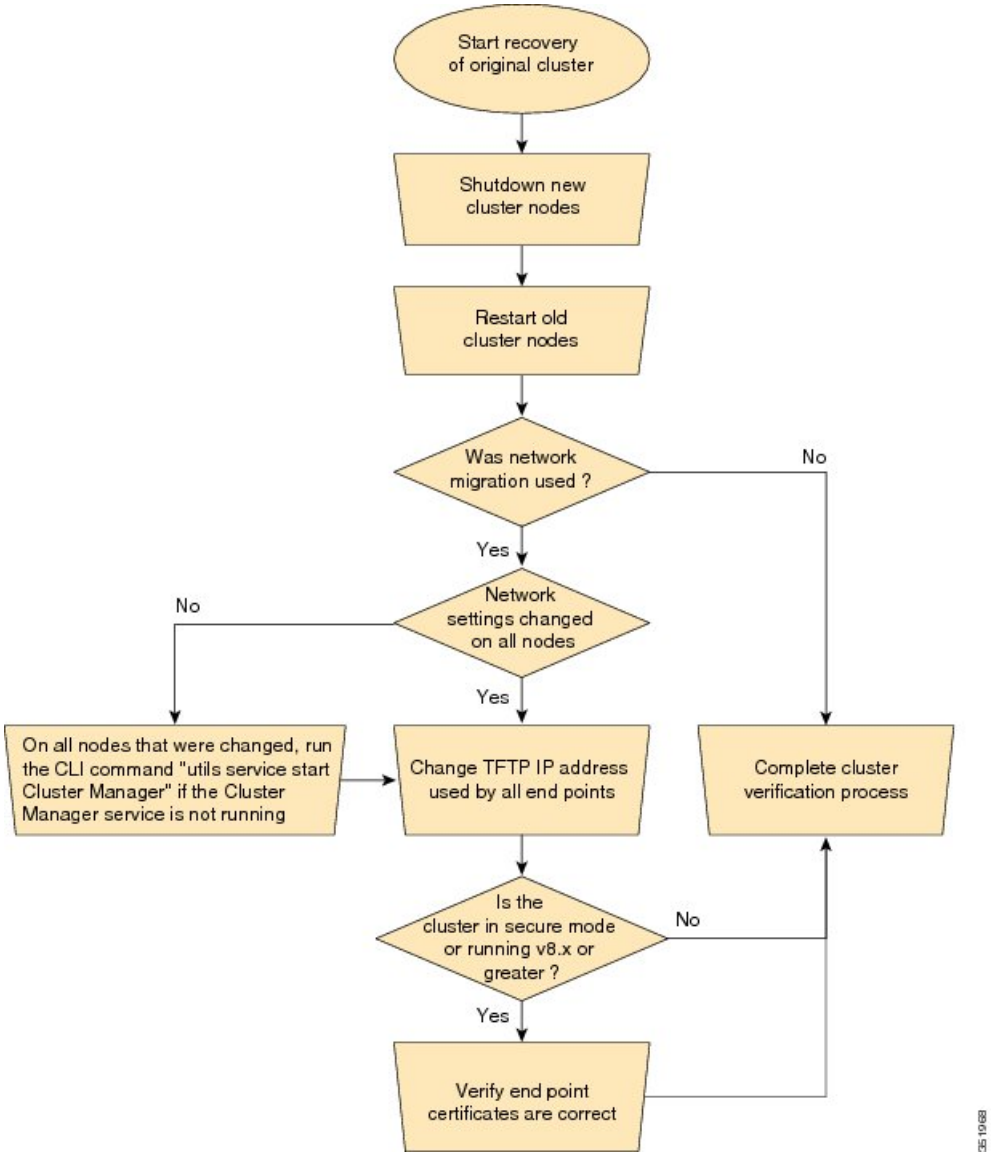
Figure 3: Flow Chart for Release 8.0.1 and later Unified CM Network Migration



Recovery of Original Cluster

Use the following procedure when a cluster fails to migrate successfully, and some nodes are installed on the new cluster.

Figure 4: Flow Chart for Recovery of Original Cluster



Check the Status of the Cluster Manager Service on All Source Nodes

The steps below are used if a migration task fails when there were network migration changes on one or more nodes. Following the failure, you may need to perform some steps to get the old cluster nodes running again.

See the flow chart above for all steps to be followed. Below are detailed steps for running the CLI command to restart cluster manager on old nodes.

Perform the following steps manually on all subscriber nodes that were supposed to have network changes (for example, hostname, IP address, or both) after all old cluster nodes are up and running.

Use cases that may require the restart of Cluster manager on source nodes are:

Use Case 1

No hostname and no IP address change on Publisher, host name change on Subscriber

The user is required to check Cluster Manager service on source Subscriber

Use Case 2

No hostname and no IP address change on Publisher, IP address change on Subscriber

The user is required to check Cluster Manager service on source Subscriber

Use Case 3

No hostname and no IP address change on Publisher, hostname and IP address change on Subscriber

The user is required to check Cluster Manager service on source Subscriber

Use Case 4

No hostname change on Publisher, IP address change on Publisher, no hostname and no IP Subscriber

The user is required to check Cluster Manager service on source Publisher

Procedure

Step 1 Enter the following CLI command at the command prompt: **utils service list**. The following output appears:

```
Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STOPPED]
```

Step 2 If Cluster Manager Service status is STOPPED, type the following command to start the service on the old subscriber node:
utils service start Cluster Manager

Upgrade Task

Create an Upgrade Task

Use the upgrade task to perform software version upgrades on a cluster. You can also use an upgrade task to install .cop files on all or a subset of servers in a cluster.

To know which applications and releases are supported for upgrade tasks, see “Supported Upgrade and Migration Tasks” and “Upgrade Paths for Export Restricted and Unrestricted Software” in the Related Topics section.

Note Cisco Prime Collaboration Deployment uses the standard upgrade process, and therefore the standard validation rules will be applied. For more information, see the application-specific documentation.

Use the Add Upgrade Task wizard to create and edit upgrade tasks.

To create or edit a new upgrade task to automatically run on one or more clusters at scheduled times, follow these steps.

Before You Begin

1. Note the supported restricted and unrestricted paths. See "Supported Upgrade and Migration Tasks" and "Upgrade Paths for Export Restricted and Unrestricted Software" in the Related Topics section.
2. Perform a cluster discovery for the cluster that you wish to upgrade, so it appears in the Cluster Inventory. See Discover a Cluster, on page 29.
3. Download the ISO files you wish to upgrade to, and use SFTP to send this file to Cisco Prime Collaboration Deployment in the upgrade folder. If you are using the upgrade task to install a .cop file, upload the .cop file to the /upgrade folder using an SFTP client.
4. For the application servers in the cluster to be upgraded, ensure that the Platform Administrative Web Service is active on that server.

Procedure

Step 1 Click the open and close navigation button and choose **Task** > **Upgrade** from the main menu.

Step 2 Click **Add Upgrade Task**.

Step 3 From the **Cluster** drop-down list, select the cluster on which the nodes to be upgraded are located.

Step 4 From the **Products** drop-down list, select the products to be upgraded.

Step 5 Select the nodes that are part of the upgrade from the list of nodes.

Step 6 Click **Next**.

Note The **Next** button is dimmed if no nodes are selected.

Step 7 Click the respective **Browse** buttons to select the upgrade files from the file server.

Note The option to select upgrade files is available only for the selected product types and applications that are currently supported in the cluster.

Step 8 Select a valid upgrade file or files.

Note Click the **Show** drop-down list to see all the available upgrade files on the file server.

Note To create an upgrade task, while selecting ISO files, ensure that the ISO files are common across all the required SFTP servers which are associated to cluster nodes. If the ISO files are not common to all the required SFTP servers which are associated to cluster nodes, the valid files do not appear even though they are valid for upgrade. To view all the ISO files, from the **Show** drop-down list, choose **All**.

Step 9 Click **Choose File**.

Step 10 Click **Next**.

Note The **Next** button is dimmed if no valid upgrade files are selected.

Step 11 Select the date and time when you want the upgrade task to begin. You have the following options to schedule upgrades:

- Select **Schedule for a specific time** to enter the date and time when you want the upgrade task to start. Any start time that you set is based on the time zone of the Cisco Prime Collaboration Deployment server as denoted by the time zone that is displayed with this option.
  Note If you schedule a task for a few minutes in the future, but do not save it until that scheduled time passes, then the task will start automatically.
- Select **Start task manually** to keep the task in a manual start.
  Note If you choose to start the task manually, a task is created, but will not start until you click the **Start task** button on the Monitoring page, or the **Start task** link on the task page.
- Select **Start task immediately upon completion of this wizard** to start the task immediately after you click **Finish**.
- If you want the system to automatically switch to the new version, choose the option **Upgrade Option to Automatically Switch to New Version after Successful Upgrade**. Otherwise, the server, or servers, will be upgraded but remain on the current version of software. In that case, the user can schedule a switch version task to switch over to the upgraded version of software.

Step 12 Click **Next**.

Step 13 Specify the sequence of steps to complete the task. You have the following options:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step. If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be performed earlier.
Down arrow	Move the step down to be performed later.

- The Pencil icon opens up an **Edit Step** window. Add nodes to be upgraded in this step from the list of available nodes. The available nodes are the ones that you chose for an upgrade.
- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.
  Important You cannot proceed to next step until you assign all the nodes.

- The **Pause task after step completes** option pauses the task after completion of this step. You must manually start the next step to complete the task.

Step 14 Click **OK**.

Step 15 Click **Next**.

Note The **Next** button remains enabled, which allows the user to click to be informed of any configuration errors.

Step 16 See the **Review** section to verify the details of the task you created. You can add notes for the task if required. The notes are saved with the task and are visible if the task is edited before completion.

Step 17 Click **Finish** to schedule the task.

Related Topics

Supported Tasks for Applications and Versions, on page 24
Upgrade Paths for Export Restricted and Unrestricted Software, on page 28

Reuse Sequence from Previous Task

The Reuse Sequence from Previous Task feature uses a previously defined task sequence in the task you are currently creating. This feature is useful for upgrade, restart, switch version, migration, and readdress tasks. It allows you to reuse a previously configured task sequence as opposed to having to rescript the sequence from scratch.

During task creation, the task wizard progresses to the sequence pane where a user can configure the ordering and pause characteristics. If there is a task in the system of similar type, the sequence from that task is presented as the default sequence.

In this case, a check box labeled **Use Last Configured Run Sequence** is visible just above the sequence table. You can check the check box to use the sequence from the previous task or leave the check box unchecked to use the default sequence that the system generates.

To be considered a task of similar type, the selected cluster, task type, and nodes in the task must match exactly. If multiple tasks meet the similar type criteria, the most recently created task is used and its sequence is presented as the default to the user.

In the case of an upgrade task, there is an additional requirement. The type of installation must be either ISO based or COP based. The COP and ISO installations can be performed with different sequencing.

Switch Versions Task

Create a Switch Versions Task

Use the switch versions task to automatically switch one or more nodes in a cluster to the upgraded or inactive version.

Use the Switch Versions Task wizard to create and edit switch versions tasks.

To know which applications and releases are supported for upgrade tasks, see “Supported Upgrade and Migration Tasks” and “Upgrade Paths for Export Restricted and Unrestricted Software” in the Related Topics section.

To create or edit a switch versions task to automatically switch one or more nodes in a cluster to the upgraded or inactive version at scheduled times, follow this procedure.

Note The Automatic Switch version option is not available on clusters which contain Unity Connection nodes. For clusters with Cisco Unity Connection, create an upgrade task and then create a switch version task to switch to the new version. You can create the switch version task after the upgrade task runs successfully.

Before You Begin

1 Perform a cluster discovery for the cluster on which you want to switch versions, so that the cluster appears in the Cluster inventory. See Discover a Cluster, on page 29. If you previously used Cisco Prime Collaboration Deployment to upgrade or migrate a cluster, the cluster should already be in the inventory.

2 For each application server in the cluster, ensure that the Platform Administrative Web Service is active on that server.

Procedure

Step 1 Click the open and close navigation button and choose **Tasks** > **Switch Versions** from the main menu.

Step 2 Click **Add Switch Versions Task**.

Step 3 From the **Cluster** drop-down list, select the cluster on which you want to switch the versions.

Step 4 Select the version to which you want all the nodes to be switched.

Note If there is more than one product, you can select the applicable versions of all the different products. You also can choose to switch the version for one product and to not switch the version for another product.

Step 5 Click **Next**.

Step 6 Select the date and time when you want the switch versions task to begin. You have the following options to schedule switch versions task:

- Select **Schedule for a specific time** to enter the date and time when you want the switch versions task to start. Any start time that you set is based on the time zone of the Cisco Prime Collaboration Deployment server as denoted by the time zone that is displayed with this option.

  Note If you schedule a task for a few minutes in the future, but do not save it until that scheduled time passes, then the task will start automatically.

- Select **Start task manually** to keep the task in a manual start.

- Select **Start task immediately upon completion of this wizard** to start the task immediately afer you click **Finish**.

  Note You can also start the task from the Monitoring page.

- If you want the server to automatically switch to the new version, check the check box next to **Automatically switch to new version after successful upgrade**.

Step 7 Click **Next**.

Step 8 Specify the sequence of steps to complete the task. You have the following options:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step. If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be performed earlier.
Down arrow	Move the step down to be performed later.

- The Pencil icon opens up an **Edit Step** window. Add the nodes on which the versions must be switched in this step from the list of available nodes. The available nodes are the ones that you chose for the switch versions task.
- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.

  Important You cannot proceed to next step until you assign all the nodes.
- The **Pause task after step completes** option pauses the task after completion of this step. You must manually start the next step to complete the task.

Step 9 Click **OK**.

Step 10 Click **Next**.

Note The **Next** button remains enabled, which allows the user to click to be informed of any configuration errors.

Step 11 Use the **Review** section to verify the details of the task that you created. You can add notes for the task if required. The notes are saved with the task and are visible if the task is edited before completion.

Step 12 Click **Finish** to schedule the task.

Related Topics

Supported Tasks for Applications and Versions, on page 24
Upgrade Paths for Export Restricted and Unrestricted Software, on page 28

Server Restart Task

To know which applications and releases are supported for upgrade tasks, see “Supported Upgrade and Migration Tasks” and “Upgrade Paths for Export Restricted and Unrestricted Software” in the Related Topics section.

Related Topics

Supported Tasks for Applications and Versions, on page 24
Upgrade Paths for Export Restricted and Unrestricted Software, on page 28

Create a Server Restart Task

Use the Restart Task wizard to create and edit restart tasks.

To create or edit a restart task to automatically restart one or more nodes in a cluster at scheduled times, follow this procedure.

Before You Begin

1 Perform a cluster discovery for the cluster you wish to restart, so that it appears in the Cluster inventory. See Discover a Cluster, on page 29.

2 For each application server in the cluster, ensure that the Platform Administrative Web Service is active on that server.

Procedure

Step 1 Click the open and close navigation button and choose **Task** > **Server Restart** from the main menu.

Step 2 Click **Add Server Restart Task**.
The Add Restart Task wizard appears.

Step 3 From the **Clusters** drop-down list, select the cluster on which you want to restart the nodes.

Step 4 From the table, select the nodes to be restarted. If you do not select any nodes, you cannot continue.

Step 5 Click **Next**.

Step 6 Select the date and time when you want the server restart task to begin. You have the following options to schedule restart tasks:

- Select **Schedule for a specific time** to enter the date and time when you want the restart task to start. Any start time that you set is based on the time zone of the Cisco Prime Collaboration Deployment server.

  Note If you schedule a task for a few minutes in the future, but do not save it until that scheduled time passes, then the task will start automatically.

- Select **Start the task manually** to keep the task in a manual start.

- Select **Start task immediately upon completion of the wizard** to start the task immediately after you click **Finish**.

Note You can also start the task from the Monitoring page.

Step 7 Click **Next**.

Step 8 Specify the sequence of steps to complete the task. You have the following options:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step. If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be prepared earlier.
Down arrow	Move the step down to be prepared later.

- The Pencil icon opens up an **Edit Step** window. In this step, add nodes to be restarted from the list of available nodes. The available nodes are the ones that you chose for a restart.
- The step to which each node is assigned appears next to the node. If a node is not assigned to any step, that node shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.
  Important You cannot proceed to the next step until you assign all the nodes.
- The **Pause task after step completes** option pauses the task after completion of this step. You must manually start the next step to complete the task.

Step 9 Click **OK**.

Step 10 Click **Next**.

Note The **Next** button remains enabled, which allows the user to click to be informed of any configuration errors.

Step 11 See the **Review** section to verify the details of the task you created. You can add notes for the task if required. The notes are saved with the task and are visible if the task is edited before completion.

Step 12 Click **Finish** to schedule the task.

Readdress Task

Create a Readdress Task

Use the readdress task change the hostname or IP address for one or more nodes in a cluster. To use the readdress feature, the servers must be Release 10.0 or later.

Note the difference between a hostname and a fully qualified domain name (FQDN) The network-level DNS default domain name of the node is combined with the hostname to form the FQDN for the node. For example, a node with hostname “cucm-server” and domain “example.com” has an FQDN of “imp-server.example.com.”

Note Cisco Prime Collaboration Deployment does not support changing the FQDN, only hostnames.

Use the Readdress Task wizard to create and edit readdress tasks.

Before You Begin

If you have not already done so, perform a cluster discovery for the cluster you wish to readdress, so that it appears in the Cluster inventory. See Discover a Cluster, on page 29.

Procedure

Step 1 Click the open and close navigation button and choose **Task** > **Readdress** from the main menu.

Step 2 Click **Add Readdress Task**.

Step 3 From the **Cluster** drop-down list, select the cluster on which you want to change the address of the nodes. Click **View Nodes** to view the Cluster nodes.

Step 4 Click **Next**.

Step 5 Click **Edit** next to a node to enter an alternate Hostname, IP Address, Subnet Mask or Gateway.

Note If DHCP is configured for a cluster, you cannot edit using the readdress task.

Step 6 Click **OK**.

Step 7 Click **Next**.

Important When you click **Next**, Cisco Prime Collaboration Deployment performs a validation test automatically. If the test on a cluster fails, the error message describes the failed test. You can continue to create the tasks, but you must resolve the errors described or the task will fail.

Step 8 Select the date and time when you want the readdress task to begin. You have the following options to schedule readdress tasks:

- Select **Schedule for a specific time** to enter the date and time when you want the readdress task to start. Any start time that you set is based on the time zone of the Cisco Prime Collaboration Deployment server as denoted by the time zone that is displayed with this option.

  Note If you schedule a task for a few minutes in the future, but do not save it until that scheduled time passes, then the task will start automatically.

- Select **Start task manually** to keep the task in a manual start.

- Select **Start task immediately upon completion of wizard** to start the task immediately afer you click **Finish**.

  Note You can also start the task from the Monitoring page.

Step 9 Click **Next**.

Step 10 Specify the sequence of steps to complete the task. You have the following options here:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
Up arrow	Move the step up to be executed earlier.
Down arrow	Move the step down to be executed later.

- The Pencil icon opens up an **Edit Step** window. Add nodes to be readdressed in this step from the list of available nodes. The available nodes are the ones that you chose for a readdress.

  Note IM and Presence Service nodes do not have an **Edit** button, since readdress is not supported on Cisco Prime Collaboration Deployment for IM and Presence Service servers.
- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, there will be a default sequencing available.

  Important You cannot proceed to next step until you assign all the nodes that were selected for this task.
- Cisco Prime Collaboration Deployment automatically inserts a Forced Pause after each sequence step in a Readdress task.
- For a readdress task, only one node can be assigned to each step. Multiple nodes cannot be combined and assigned in a single step.

Step 11 Click **OK**.

Step 12 Click **Next**.

Note The **Next** button remains enabled, which allows the user to click to be informed of any configuration errors.

Step 13 See the **Review** section to verify the details of the task you created. You can add notes for the task if required. The notes are saved with the task and are visible if the task is edited before completion.

Step 14 Click **Finish** to schedule the task.

Run a Readdress Task

If you scheduled the task to start at a later date, or if you chose Manual Start, then the task will be listed in the task list but will not start yet.

For a task that was scheduled for manual start, click the **Start** button that is associated with this task to begin the task.

While the readdress task is running, if there is more than one server to be readdressed in the task, some user operations are needed. The readdress task sequence automatically inserts a Forced Pause into the sequence after the address of a server is changed.

This allows the user to perform any manual steps (for example, changes in DNS) and to check that the phones associated with the server successfully registered, and the system is successfully replicating, before Resuming the readdress task.

For more information, see *Administration Guide for Cisco Unified Communications Manager*.

Before You Begin

Important Before running a readdress task, you may need to perform certain steps (for example, updating entries on the DNS server).

It is very important that you read *Administration Guide for Cisco Unified Communications Manager* before you run the readdress task.

Post Readdress Task

When you determine that the server successfully changed the address, go to the Cisco Prime Collaboration Deployment GUI and click **Resume** to resume the task.

The Cisco Prime Collaboration Deployment server proceeds to the next server in the sequence to be readdressed. Repeat the steps of waiting for the forced pause, checking the server state, and resuming the task, when the server readdress is verified.

Install Task

Use this task to fresh install a cluster containing Unified Communications Manager or IM and Presence Service servers. You cannot use this task to add a new server to an existing cluster.

Create an Install Task

Before You Begin

1 VMware—Deploy the hardware for the new cluster and install ESXi

Note Make sure that the host with the Cisco Prime Collaboration Deployment VM and the host with the application VMs use the required Virtualization Software License. See Virtualization Software License Types, on page 4.

2 ISO files—Download the necessary OVA and ISO images for target release, and use SFTP transfer the ISO files to the `/fresh_install` directory of Cisco Prime Collaboration Deployment.

Note The ISO file must be bootable.

Note Do not edit the file name of the bootable ISO that is being used for a PCD task.

3 VMware—Deploy Cisco-recommended OVA to create the VMs for the nodes to be installed. Create the appropriate number of target virtual machines on your ESXi hosts (one new virtual machine for each server to be installed in the cluster) using the Cisco OVAs that you downloaded in Step 2. Configure the network settings on new VMs.

4 Cisco Prime Collaboration Deployment GUI—Add the ESXi Hosts that contain your virtual machines to the Cisco Prime Collaboration Deployment inventory. For information about adding and ESXi host to Cisco Prime Collaboration Deployment, see Add an ESXi Host Server, on page 32.

5 Cisco Prime Collaboration Deployment GUI—Define the new installation cluster (click the open and close navigation button and choose **Inventory** > **Clusters**) to define the nodes to be installed, and their associated virtual machines. (See Add New Cluster for Fresh Install, on page 34.)

6 Cisco Prime Collaboration Deployment GUI—Setup Email Notification (Optional)

- Click the open and close navigation button and choose **Administration** > **Email Notification**.
- When email notification is set up, the Cisco Prime Collaboration Deployment server emails the error conditions that may occur during the migration task.

7 Cisco Prime Collaboration Deployment GUI—Create the Install task.

8 Be sure to enter the IP addresses or hostnames of the cluster nodes to be installed into your DNS server before you create the install task.

Add Install Task

Follow this procedure to automatically install one or more nodes in a cluster at scheduled times.

Procedure

Step 1 Click the open and close navigation button and choose **Task** > **Install** from the main menu.

Step 2 Click **Add Install Task**.

Note If you have no Install tasks, a **Cluster Installation** popup window appears with the prerequisites to run the wizard. Click **Close** to close the popup window.

Step 3 From the **Installation Cluster** drop-down list, select the cluster on which the nodes to be installation are located.

Step 4 Click **Next**.

Step 5 Click the respective **Browse** buttons to select the Unified Communications Manager Installation file and the Cisco Unified Presence Installation file from the server.

Note The ISO file is visible here only if it was placed in the directory under `/fresh_install`, uploaded through a standard SFTP client (Admin Name: adminsftp, Password: Administration password). For more information, see the task management information at the beginning of this section.

Note By default, only files that can be installed on the selected nodes are displayed. The option to select install files is available only for the selected product types and applications that are currently supported in the cluster.

Step 6 Click **Choose File**.

Step 7 Click **Next**.

Note The **Next** button is dimmed if no valid upgrade files are selected.

Step 8 Select the date and time when you want the upgrade task to begin. You have the following options to schedule upgrades:

- Select **Schedule for a specific time** to enter the date and time when you want the upgrade task to start. Any start time that you set is based on the time zone of the Cisco Prime Collaboration Deployment server as denoted by the time zone that is displayed with this option.

  Note If you schedule a task for a few minutes in the future, but do not save it until that scheduled time passes, then the task will start automatically.

- Select **Start task manually** to keep the task in a manual start.

- Select **Start task immediately upon completion of this wizard** to start the task immediately afer you click **Finish**.

  Note You can also start the task from the Monitoring page.

Step 9 Click **Next**.

Step 10 Specify the sequence of steps to complete the task. You have the following options:

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step. If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be performed earlier.
Down arrow	Move the step down to be performed later.

- The Pencil icon opens up an **Edit Step** window. Add nodes to be installed in this step from the list of available nodes. The available nodes are the ones that you chose to install in this cluster.

- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.

- When you assign all the nodes to a step, a default sequencing is available.

  Important You cannot proceed to next step until you assign all the nodes.

- If you are installing Cisco Unified Communications Manager between Releases 10.0(1) and 10.5(1), the task is paused after publisher node is installed completely. You must enter details of subscriber nodes

into the publisher node before you manually start the next step. Cisco Unified Communications Manager Release 10.5(2) onward does not pause during a fresh installation; the install task continues automatically.

Step 11 Click **OK**.

Step 12 Click **Next**.

Note The Next button remains enabled, which allows the user to click to be informed of any Misconfiguration.

Step 13 See the **Review** section to verify the details of the task you created. You can add notes for the task if required. The notes are saved with the task and are visible if the task is edited before completion.

Step 14 Click**Finish** to schedule the install task.

Important When you create a fresh install cluster with both Unified Communications Manager and IM and Presence Service nodes, be sure to indicate which IM and Presence server is the publisher. Later, when the task is running, and it pauses after the Unified Communications Manager publisher installation to allow for entry of the subscriber nodes into the Unified Communications Manager publisher (**System** > **Server** GUI menu), it is important that the IM and Presence Service publisher be the first IM and Presence Service server added to this list. This ensures that IM and Presence Service is installed as the first node.

Note The Unified Communications Manager publisher requires that all subsequent servers in the cluster be added to the Cisco Unified Communications Manager Administration GUI, after the Publisher is installed. Because of this requirement, when you create an install task, Cisco Prime Collaboration Deployment automatically inserts a Forced Pause in the sequence steps after the Unified Communications Manager (Releases from 10.0(1) to 10.5(1)) publisher is installed.

Run an Install Task

If you scheduled a task to start at a later date or if you chose Manual Start, the task is listed in the Task list, but has not started yet. In this case, a validation button is associated with the install task. Click **Validation** to check the task before you run it. By running validation before you start the task, you are alerted to any potential problems with the task (such as a missing ISO file or VMs not in the Off state). You can then fix these issues before you start the task.

Note Clicking the **Validation** button will not start the task; this button only checks the resources to be used when the task starts.

For a task that was scheduled for manual start, click the **Start** button that is associated with this task to begin the task.

When a fresh install task includes more than just one server, some user interaction is required while the task is running. The installation task automatically installs the Unified Communications Manager publisher first, and then the task sequence will have a forced pause. This forced pause stops the install task to allow the user to go to the Unified Communications Manager GUI of the newly installed publisher, and add the other servers in the cluster into the **System** > **Servers** window. To define the subsequent nodes, click **Add New** and configure the server.

After all the subscribers to be installed in this cluster (Unified Communications Manager subscribers, IM and Presence Service publisher and IM and Presence Service subscribers) are added to the Unified Communications Manager publisher GUI, return to the Monitoring page in the Cisco Prime Collaboration Deployment GUI

and click the **Resume** button for the install task to resume. The install task continues and installs the Unified Communications Manager or IM and Presence Service software on the subsequent server (or servers).

Cancel Install Task

Use this procedure to cancel a fresh install task or an existing installation in a migration task.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Task** > **Install** from the main menu.
The existing install tasks appear in the **Task List** section.

Step 2 Select an existing install task and click **Cancel**.

Note If you cancel the currently running install task, you will have to delete the virtual machine and then recreate it.

The virtual machine of the selected install task turns off and the task status is displayed as **Canceled**.

Post-Install Task

After the install task, no further actions are required. The new cluster is ready for use.

Edit and Expand Cluster Support

If you deployed a Cisco Unified Communications Manager cluster, the Edit and Expand Cluster support feature in Cisco Prime Collaboration Deployment eliminates migration issues and barriers. You can perform the following actions:

- Add IM and Presence Service to an existing Unified Communications Manager cluster.
- Add new nodes to the existing cluster—for example, add subscriber nodes.
- Select nodes from a cluster to perform installation.

This feature works with only a previously installed 10.x or later system and uses the Fresh Install Task to add the nodes.

Note After you add and install new nodes to an existing cluster, if you later perform the Discovery task, the entire cluster with the new nodes is discovered.

Edit or Delete a New Install Cluster

Edit or delete an added new node that has not yet been installed. A node that has not been installed appears active.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **Clusters**.

Step 2 Click a cluster that has the cluster type as **New Install** and click **Edit**.

Step 3 In the Specify Cluster Name section, view the pre-populated cluster name, and click **Next**.

Step 4 In the Add Virtual Machines section, select a node from the existing nodes, and click **Edit**.
The **Add Node** window appears.

Step 5 In the **Add Node** window, edit the node details, and click **OK**.

Step 6 In the Configure Cluster Wide Settings section, edit the OS administration credentials, application credentials, security password, SMTP settings, and certificate information for all nodes of a cluster, as required, and click **Next**.

Step 7 (Optional) In the Configure DNS Settings section, edit the DNS settings for the migration cluster nodes, and click **Next**.

Note If the previous nodes in the cluster have the same values for DNS and domain, then the value from the other nodes becomes the default value for the new nodes and is auto-populated. If the previous nodes have multiple values for DNS or domain, then no default value is applied.

Step 8 In the Configure NTP Settings section, edit the configuration of the NTP servers for the nodes in a cluster, and click **Next**.

Note The changes you make in this section apply to publisher node only.

Step 9 (Optional) In the Configure NIC Settings section, choose a server, and enter an MTU size between 552 and 1500, click **Apply to Selected**, and then click **Next**.

Step 10 In the Configure Time Zones section, select a node, edit the region and time zone from the Region and Time Zones list boxes, click **Apply to Selected**, and then click **Finish**.

Note If the previous nodes in the cluster have the same values for time zone, then the value from the other nodes becomes the default value for the new nodes and is auto-populated. If the previous nodes have multiple values for time zone, then no default value is applied.

The changes are saved. You can install one or multiple nodes in a cluster. See Add Install Task, on page 58 for details.

Edit or Delete a Discovered Cluster

You can edit or delete a node that has not yet been installed. A node that has not been installed appears active and the installed nodes appear inactive.

Note After you add or install a new node, you cannot delete the node with this feature. You must delete the node from an existing installed cluster by using your application administration web page or the CLI.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **Clusters**.

Step 2 From the Cisco Prime Collaboration Deployment application, select **Inventory** > **Clusters**.

Step 3 Click a cluster that has the cluster type as **Discovered** and click **Edit**.

Step 4 In the Specify Cluster Name section, enter the cluster name, and click **Next**.

Note If the discovered cluster is already installed, the cluster name is non-editable.

Step 5 In the Add Virtual Machines section, select a node from the existing nodes that has not been installed, and click **Edit**.
The **Add Node** window appears.

Step 6 In the **Add Node** window, edit the node details, and click **OK**, and then click **Next** in the Add Virtual Machines section.

Note If you add a new node to an existing cluster, the new nodes cannot use the **Publisher** function

Step 7 In the Configure Cluster Wide Settings section, view the OS administration credentials, application credentials, security password, SMTP settings, and certificate information for all nodes of a cluster and click **Next**.

Note The fields in this section are editable only if the cluster type is **New Install**.

Step 8 (Optional) In the Configure DNS Settings section, edit the DNS settings for the migration cluster nodes, and click **Next**.

Note If the previous nodes in the cluster have the same values for DNS and domain, then the value from the other nodes becomes the default value for the new nodes. If the previous nodes have multiple values for DNS or domain, then no default value is applied.

Step 9 In the Configure NTP Settings section, view the configuration of the NTP servers for the nodes in a cluster, and click **Next**.

Note The fields in this section are non-editable.

Step 10 (Optional) In the Configure NIC Settings section, edit the server details for the uninstalled nodes, enter an MTU size between 552 and 1500, and then click **Next**.

Step 11 In the Configure Time Zones section, select a node, edit the region and time zone from the Region and Time Zones list boxes, click **Apply to Selected**, and then click **Finish**.

Note If the previous nodes in the cluster have the same values for time zone, then the value from the other nodes becomes the default value for the new nodes. If the previous nodes have multiple values for time zone, then no default value is applied.

The changes are saved. You can install one or multiple nodes in a cluster. See Add Install Task, on page 58 for details.

Monitor Task Status

Use the Monitoring page to view the status of tasks in Cisco Prime Collaboration Deployment.

Note For a description of the information that is available through the Monitoring page, see Monitoring View Elements, on page 80.

Procedure

Step 1 Click the **Monitoring** link on the main menu to view the Monitoring page.

Step 2 The column on the left side of the Monitoring page lists each task and an icon that shows its current status. Also shown is the type of task (Migrate, Upgrade, Install, and so on), and the cluster nickname for the task. The task start time is also shown. Click the task in this left column to view the detailed data for that task in the panel on the right.

Step 3 The upper right section of the page provides the following data:

- Status
- Start time
- Task data (for example: cluster nickname and ISO name)

Click **View Log** to see the detailed log messages for the task. If you see any errors or warnings in this log, refer to the Troubleshooting section more information.

In the upper right are buttons that you use to perform various operations on the task. For example, if the task is paused, click the **Resume** button to resume the task.

A button will appear if it is valid for the current state of the task. For example, after a task is finished, it will not have a **Cancel** button, but instead will have a Delete button (if you wish to remove the data for the task).

Step 4 The bottom right section of the page provides detailed steps for the task, along with the status for that step. Click on the triangle that corresponds to a step to expand the step description.
Each step also has a View Log link, to show the log messages for that step.

Note The Monitoring page refreshes automatically every 3 minutes. To deactivate automatic refresh, click the **Disable** button.

Action Buttons on the Monitoring Page

- **Start—**This button appears if a task is created with the "Start Task Manually" option. The task starts after you click the Start button.
- **Cancel—**Cancel the task. This button appears when a task is in the scheduled or running state. If the task has already started, this button does not undo any steps that are already complete, but it will stop the task as soon as possible.
- **Delete—**Delete the task from the system. This removes the task and all its history.
- **Resume—**This button appears when a task is in a paused state. It allows the user to resume the task at the next step.
- **Retry—**This button appears when the task is in a "Paused due to error" state. Clicking this button retries the last step of the task that failed because of an error.

Automatic Refresh

The Monitoring page refreshes automatically every 3 minutes. To deactivate automatic refresh, click the **Disable** button in the top left corner of the Monitoring page.

Administration Tools

Email Notification

The Email Notification feature sends email notifications to you that contain details about certain task events. You can choose whether the system sends emails for all standard task events (such as when task is scheduled, started, successful, paused, failed and canceled), or for only task errors. Emails are sent for all types of tasks—cluster discovery, upgrade, migration, switch version, restart, fresh install, and readdress.

You can choose to send an email notification to a user after the value that is configured in the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field from the **Audit Log Configuration** window is reached. The email notification informs the user to take back up of the audit log files because they will be deleted or overwritten.

When Email Is Sent

If you choose to receive email notifications in **Standard mode**, an email message is sent when a task enters any of the following states:

- Scheduled
- Failed to Schedule
- Started
- Successful
- Failed
- Canceled
- Canceling
- Failed to Cancel
- Paused on Error
- Paused
- Paused – Required

If you choose to receive email notifications in **Error only mode**, an email message is sent when the task enters the following states:

- Failed to Schedule
- Failed
- Failed to Cancel

- Paused on Error

SFTP Datastore

The Cisco Prime Collaboration Deployment server serves as a local SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP) server that is used to store the ISO and COP files to be used by upgrade, fresh install, and migrate tasks.

Note These procedures describe how to place files on the Cisco Prime Collaboration Deployment server using Linux. You can push a file from a Linux machine for SFTP client.

Migration or Fresh Install Tasks

Follow this procedure to send the ISO file to the Cisco Prime Collaboration Deployment server using the adminsftp account and Cisco Prime Collaboration Deployment GUI (or CLI password with any SFTP client).

Procedure

Step 1 From a Linux shell, type `sftp adminsftp@<Cisco Prime Collaboration Deployment server>` and then provide the password (the same in both the CLI and GUI).

Step 2 Change the directory to the `fresh_install` directory.

Example:
From a Linux shell, type `cd fresh_install` and press Return.

Step 3 Upload the ISO file.

Example:
Type `put UCSInstall_UCOS_10.0.x.xxx.sgn.iso`.

Upgrade Task

Follow this procedure to use SFTP to upload ISO or COP files that will be used for upgrade tasks on the Cisco Prime Collaboration Deployment server.

Procedure

Step 1 From a Linux shell, type `sftp adminsftp@<Cisco Prime Collaboration Deployment server>` and then provide the password (the same in both the CLI and GUI).

Step 2 Change the directory to the `upgrade` directory.

Example:
From a Linux shell, type `cd upgrade` and press Return.

Step 3 Upload the ISO file or COP file.

Example:
Type `put UCSInstall_UCOS_10.0.x.xxx.sgn.iso`.

Verify or View an ISO Filename

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.

Step 2 On this page, you can view and manage files that are stored on the SFTP datastore of this Cisco Prime Collaboration Deployment server.
It displays the filename of the ISO and COP files that are stored on the server, and where they are located in the directory (for example: fresh_install or upgrade).

Delete ISO or COP Files

Use the following procedure to delete ISO or COP files on a Cisco Prime Collaboration Deployment SFTP server using the Cisco Prime Collaboration Deployment GUI.

Procedure

Step 1 Log in to Cisco Prime Collaboration Deployment.

Step 2 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.

Step 3 Check the check box next to the ISO or COP file.

Step 4 Click **Delete**.

Important We recommend that you periodically delete ISO or COP files that are no longer needed to save space, especially before upgrading the Cisco Prime Collaboration Deployment server software.

Remote SFTP Server Support

The remote SFTP server support feature leverages Cisco Prime Collaboration Deployment for upgrades. Use of this feature avoids the issues that are caused by large application image files streamed over WAN that are only supported by Cisco Prime Collaboration Deployment 11.0(1) and later.

Examples of where this feature is useful are listed as follows:

- Geographically distributed deployments, such as multi-site distributed IP Telephony with multiple clusters at separate sites from the Cisco Prime Collaboration Deployment virtual machine.
- Clustering over WAN (CoW), where the application virtual machines are at different sites than the Cisco Prime Collaboration Deployment virtual machine.
- Deployments where Cisco Prime Collaboration Deployment is in central data center; however Cisco Unified Communications Manager clusters are remote over the WAN.

These SFTP servers used for the upgrade of Cisco Unified Communications Manager are same as the SFTP servers that are used for the upgrade of Cisco Unified Communications Manager. Following is the list of the supported SFTP servers that are used for the upgrade:

- Open SSH
- Cygwin
- Titan

Note The remote SFTP server support is available for upgrade task only and no other task types, including the migration task.

Add Remote SFTP server

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.
The **SFTP Servers/Datastore** table on this window shows the PCD details by default.

Step 2 From the **SFTP Servers/Datastore** table, click **Add Server**.
The **Add SFTP Server** window appears.

Step 3 In the **Address and access credentials** section, enter values in the **IP / Host Name**, **Username**, and **Password** fields.

Step 4 In the **Path to Datastore Directory on Server** section, click a **Add Directory** button to add a value in the **Directory** field.

Note For an upgrade, ensure that a directory includes .iso datastore files.

Step 5 (Optional) In the **Additional Information** section, enter description in the **Description** field.

Step 6 Click **Add**.

Note If the SFTP server is not added, you get any of the following error messages:

- **Connection Timeout—**Indicates that the connection to SFTP server failed due to timeout.
- **Login Failure—**Indicates that the login to the SFTP server failed.
- **Directory Not Found—**Indicates that the directory that you selected is not found on the SFTP server.
- **Directory Already Entered—**Indicates that the directory that you selected already exists in the list of directories. You can view the list of available directories by clicking the **Add Directory** button.
- **Directory Already Exists—**Indicates that the directory that you entered already exists in the list of the SFTP servers.
- **Mandatory Fields Missed—**Indicates that you did not enter values in the mandatory fields.
- **Mentioned Server Could Not Be Located—**Indicates that the server that you entered is not configured with DNS. This error message appears if you enter host name instead of IP address.

The **SFTP Servers/Datastore** table shows the remote SFTP server that you added. The **SFTP/Datastore Files** table shows the list of files from the remote SFTP server and from Cisco Prime Collaboration Deployment. In addition, the existing Cisco Prime Collaboration Deployment server is added automatically and the files in the `upgrade` and `fresh_install` folders in the Cisco Prime Collaboration Deployment server appear by default in the **SFTP/Datastore Files** table.

Associate Nodes to Remote SFTP Server

Before You Begin

- Add an SFTP server.
- Ensure that the cluster node you choose to associate to an SFTP server is not in the **Scheduled**, **Running**, or **Wait_for_manual_start** states.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **Clusters**.
The **Clusters** window appears.

Step 2 Click **Discover Cluster** button to search for the existing clusters. To discover a cluster, see the Discover a Cluster, on page 29 procedure.

Step 3 From the available cluster nodes in the **Cluster Nodes** table, click **Edit** for a cluster node.
The **Edit Node** window appears.

Step 4 From the **SFTP Server** drop-down list, choose an SFTP server.
By default, this field shows the localhost option as the SFTP Server.

Step 5 Click **OK**.

The SFTP server is associated with the cluster node that you selected and the details appear in the **SFTP Server** column of the **Cluster Nodes** table.

Edit Remote SFTP Server

For the existing remote SFTP server, you can edit the details, such as username, password, or description. You can also add multiple directories to the remote SFTP server while editing other field values.

Before You Begin

- Ensure that a cluser node is not associated with remote SFTP server directory that you choose to edit.
- Ensure that no upgrade task is associated with the SFTP server.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.
The **SFTP Servers/Datastore** table on this window shows the PCD details by default.

Step 2 From the available SFTP servers in the **SFTP Servers/Datastore** table, click **Edit** for an SFTP server.
The **Edit SFTP Server** window appears.

Step 3 Edit the values for the fields in the **Address and access credentials**, **Path to Datastore Directory on Server**, and **Additional Information** sections.
In **Path to Datastore Directory on Server** section, by clicking the **Add Directory** button, you can edit an existing directory and also add multiple directories.

Step 4 Click **Save**.

Delete Remote SFTP Server

You can delete one or multiple remote SFTP servers that are available in the Cisco Prime Collaboration Deployment application. However, you cannot delete any datastore.

Before You Begin

- Ensure that no upgrade task is associated and running with the cluster node that uses the SFTP server that you choose to delete.
- Disassociate the cluster nodes from the SFTP server that you choose to delete.

Note You can disassociate a cluster node even if no upgrade task is associated and running with the cluster node that uses the SFTP server that you selected to delete.

- Ensure to change the node association of the SFTP server, which you choose to delete, from `remote/external` SFTP server to the `localhost` SFTP server.

Note If you do not change the node association from `remote/external` SFTP server to the `localhost` SFTP server, the association of cluster nodes changes to the `localhost` SFTP server from the remote SFTP server and the remote SFTP server that you selected is deleted.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.
The **SFTP Servers/Datastore** table on this window shows the PCD details by default.

Step 2 From the available SFTP servers in the **SFTP Servers/Datastore** table, check the check box of one or multiple remote SFTP servers that you want to delete.

Step 3 Click **Delete**.

Delete Local SFTP/Datastore ISO files

You can delete ISO and COP files from the SFTP server running locally in the Cisco Prime Collaboration Deployment virtual machine. However, you cannot delete ISO files from the remote SFTP server.

Before You Begin

Ensure that the SFTP and datastore ISO files that you choose to delete are not associated with the upgrade in these states—**Scheduled**, **Running**, or **Wait_for_manual_start**.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Inventory** > **SFTP Servers and Datastore**.
The **SFTP Servers/Datastore** table on this window shows the PCD details by default.

Step 2 From the available SFTP and datastore files in the **SFTP/Datastore Files** table, check the check box of one or multiple remote SFTP and datastore files that you want to delete.

Note You cannot delete remote SFTP files.

Step 3 Click **Delete**.

Disk Space Warning Level

Use this feature to view and configure a disk space warning level for tasks through the **Disk Space Warning Level Configuration** window. When the available disk space value drops below the value that you assign as the warning level disk space, the system warns you that it is running out of disk space to perform tasks.

Configure Disk Space Warning Level

Use this procedure to configure the available disk space threshold where the system warns you that it is running out of disk space to perform tasks.

Note Disk space warning level is applicable and is validated for migration and install tasks. This level is also validated each time you log in to Cisco Prime Collaboration Deployment.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **Disk Space Warning Level**.
The **Disk Space Warning Level** window appears showing the total disk space and the available disk space.

Step 2 View the total disk space and the available disk space in the **Total Disk Space (GB)** and **Available Disk Space (GB)** fields.

Step 3 Enter the value that you want to assign for the **Warning Level Disk Space (GB)** field.
You can click the information link to check if the space value you entered is available for use on the server.

Step 4 Click **Save**.

Step 5 (Optional) Click **Reset**.
The page is reset with the default values.

Audit Log Configuration

Use this feature to configure audit logs through Cisco Prime Collaboration Deployment interface for local and remote syslog servers. The audit logs are sent to the syslog server in the TCP mode. You can configure audit logs through the **Audit Log Configuration** window and perform the following tasks:

- Configure application audit event levels
- Configure remote Syslog server name or IP address
- Enable or disable audit logs
- Enable or disable log rotation
- Configure maximum number of files
- Configure file size
- Configure warning threshold level for log rotation

Configure Audit Logs

Use this procedure to configure audit logs for local and remote syslog server through the Cisco Prime Collaboration Deployment application.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **Audit Log Configuration**.

Step 2 Choose one of the options from the **Application Audit Event Level** drop down list to configure an audit level.

Step 3 Enter the name of remote syslog server or the IP address for the **Remote Syslog Server Name / IP** field so that the audit logs are logged into this remote server.

Step 4 (Optional) Check or uncheck the **Enable Local Audit Log** check box to enable or disable the local audit log.

- When you check this field, the audit events are logged in the local server. When you uncheck this field, audit events are not logged in the local server.
- When you check this field, the **Enable Log Rotation** field becomes active.

Step 5 (Optional) Check or uncheck the **Enable Log Rotation** check box to enable or disable the log rotation.

Note You can configure this field if **Enable Local Audit Log** is enabled.

When you check this field, you can configure the **Maximum No of Files**, **Maximum File Size(MB)**, and **Warning Threshold for Approaching Log Rotation Overwrite(%)** fields. When you uncheck the **Enable Local Audit Log** field, the default values of these fields are not applicable as they are inactive.

Step 6 Enter an integer value for the **Maximum No of Files** field to configure the maximum number of files that can be created on the server.

Step 7 Enter a value for the **Maximum File Size (MB)** field to configure the maximum file size of each log that is created on the server.

Step 8 Enter the warning threshold value for the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field.

Step 9 Click **Save**.

Step 10 (Optional) Click **Reset**.
The page is reset with the default values.

Customized Logon Message

Use this feature to display the alerts or warning messages while signing in to the Cisco Prime Collaboration Deployment application. You can configure the alerts or warning messages through the **Customized Logon Message** window and perform the following tasks:

- Upload a file with customized login message
- Enable user acknowledgment

Configure Customized Logon Message

Use this procedure to configure customized logon messages when a user signs into the Cisco Prime Collaboration Deployment application.

Procedure

Step 1 From the Cisco Prime Collaboration Deployment application, click the open and close navigation button and choose **Administration** > **Customized Logon Message**.

Step 2 For the **Upload File** field, browse to the location of file that includes the customized logon message.

Step 3 (Optional) Check or uncheck the **Require User Acknowledgement** check box to enable or disable user acknowledgment for the file that the user receives.
If this field is enabled, users get an acknowledgment as an alert message on the Cisco Prime Collaboration Deployment sign-in page after they sign out for the first time from the same web browser instance.

Step 4 Click **Upload File**.
The file with the customized logon message is uploaded and a pop-up appears showing the file upload status.

Step 5 (Optional) Click **Delete**.
The file with the customized logon message is deleted and a pop-up appears showing the file deletion status.

FIPS 140-2 Compliance

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow. A cryptographic module is a set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Certain versions of Unified Communications Manager are FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance. Cisco Prime Collaboration Deployment meets FIPS 140-2 requirements by using Cisco-verified libraries.

For information about which releases are FIPS-compliant and to view their certifications, see http://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

For details on EnhancedSecurityMode, see EnhancedSecurityMode Support, on page 74.

Note Elliptic Curve Digital Signature Algorithm (ECDSA) ciphers are not supported in Cisco Prime Collaboration Deployment. Hence, during TLS connection, the server does not negotiate the ECDSA certificates even though the **show cert list own** CLI command may show the ECDSA self-signed certificate.

EnhancedSecurityMode Support

Once you enable EnhancedSecurityMode, the following system enhancements are enabled by default:

- Stricter credential policy is implemented for user passwords and password changes
- TCP becomes the default protocol for remote audit logging
- FIPS mode is enabled

Enabling EnhancedSecurityMode does not enable these features by default and you have to configure them separately.

- Remote audit logging—All audit logs and event syslogs should be saved both locally and to a remote syslog server.
- System logging—All system events such as CLI logins and incorrect password attempts must be logged and saved.

Credential Policy for EnhancedSecurityMode

Once the EnhancedSecurityMode is enabled, a stricter credential policy for password changes is implemented automatically for Cisco Prime Collaboration Deployment. This mode uses the following default requirements for password changes:

- Password length should be between 14 to 127 characters.
- Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Any of the previous 24 passwords cannot be reused.
- Minimum age of the password is 1 day and Maximum age of the password is 60 days.
- Any newly generated password's character sequence should differ by at least 4 characters from the old password's character sequence.

Once this mode is enabled, the system enforces a stricter credential policy for all password changes automatically.

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment

As part of EnhancedSecurityMode requirement, audit framework is introduced in Cisco Prime Collaboration Deployment. The audit framework includes audit activities, which are both in local server and remote server. The login sessions are limited for each user based on the CLI command configuration in the EnhancedSecurityMode.

Note By default, auditing is not enabled in Cisco Prime Collaboration Deployment. If you wish to have audit logs, you can enable auditing with or without being in FIPS mode or EnhancedSecurityMode.

Audit Framework and Audit Activities

As part of audit framework, you can configure logging audit details from the Cisco Prime Collaboration Deployment application.

You can configure these details from the following options:

- **Logout** button
- **Email Notification** window

- **NAT Settings** window
- **Disk Space Configuration** window
- **Audit Log Configuration** window
- **Customized Logon Message** window

If you configure audit logs for any of the above options, the updates made in the field values trigger an audit log into the local server or remote syslog server. Examples of audit log activities include enabling log rotation, configuring maximum number of files and file size, and configuring addition and modification of log files.

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment

You can use the command line interface (CLI) to enable EnhancedSecurityMode in Cisco Prime Collaboration Deployment. To enable this mode, create a status file and run the scripts for applications. The applications read the status file and respond accordingly when the system is restarted.

For Cisco Prime Collaboration Deployment to work in EnhancedSecurityMode, following requirements are met:

- Sign in banner appears prior to interface sign-in prompt
- The Department of Defense (DoD) sign-in banner appears prior to console sign-in prompts
- File Transfer Protocol Secure (FTPS) or File Transfer Protocol (FTP) service and SSH are configured with the DoD sign-in banner
- The banner appears on the screen until a user signs on for further access
- Audit tools are secured from unauthorized modification
- Audit records are used through reports
- New password is verified, as per EnhancedSecurityMode credential policy, when a user changes password

Note For credential policy for EnhancedSecurityMode, see Credential Policy for EnhancedSecurityMode, on page 75.

Re-encryption through AES

The encryption and decryption of application passwords is done in the `platformConfig.xml` file. During installation, the application password is re-encrypted through the Advanced Encryption Standard (AES) algorithm and is saved in the `platformConfig.xml` file.

Limited Number of Sign-in Sessions

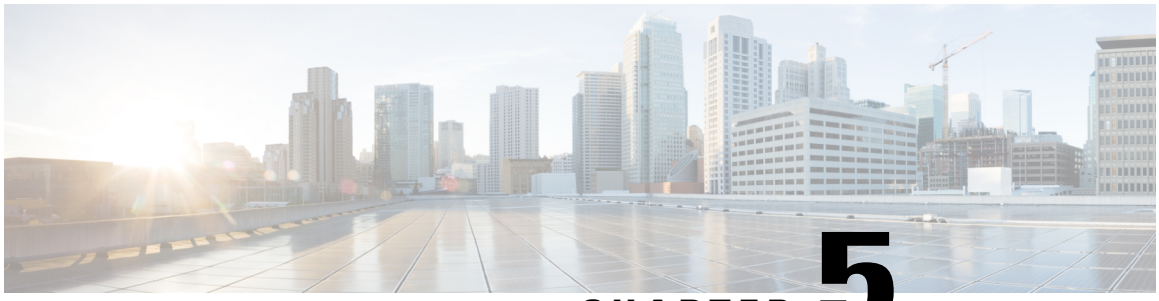
An administrator can configure the sign-in session limit for each user. A user can sign in to the Cisco Prime Collaboration Deployment application through multiple windows and web browsers up to the configured number of sign-in sessions. If a user exceeds the limit of configured the number of sign-in sessions, an error message appears on the sign-in page and the user is not allowed to sign in.

An administrator can configure the limit of sign-in sessions through the following CLI command:

set session maxlimit <value>

Where the default value is 10 and maximum value is 100.

Note When users exceed the limit of configured number of sign-in sessions, they must sign out from the application in that session and sign in to another session. In case the session closes due to abrupt exit from web browser, users need to restart the Tomcat server on Cisco Prime Collaboration Deployment to allow sign-in to the new session.



CHAPTER 5

Cisco Prime Collaboration Deployment Administrative Interface Elements

- Common Administrative Interface Elements, page 79
- Monitoring View Elements, page 80
- Tasks View Elements, page 84
- Inventory View Elements, page 113
- Administration View Elements, page 122

Common Administrative Interface Elements

The following elements are common to all views in the Cisco Prime Collaboration Deployment administration interface.

Setting	Description
Open and close navigation button	Provides you access to navigate to menus, which appear in a vertical pane. Click this button view and hide the menus. **Note** When you sign in to the application for the first time, a transparent grey screen appears indicating this button. This screen also shows a pop-up message to turn off the indication.
Search and Indexing	Displays the search text box to allow search in the application. It also displays the options Cisco Prime Collaboration Deployment as index. **Note** To view the search option, click the open and close navigation button.
About	Provides the version of the Cisco Prime Collaboration Deployment. This setting also includes copyright and trademark information.
Logout	Exits from the server.
Help	Provides context-sensitive help information.

Setting	Description
Information ("i" button)	Provides information about the current page that you are viewing.
Getting Started (flag button)	Provides information about getting started to perform system-level tasks on the server.

Monitoring View Elements

After a task is scheduled, you can monitor, and control the tasks by using the Monitoring page.

Setting	Description
Task Queue	A list of all the tasks contained in Cisco Prime Collaboration Deployment. This list can include any of the following tasks: • Scheduled • Canceled • Started • Paused • Paused due to Error • Successful • Failed • Upgrade Tasks • Switch Version Tasks • Server Restart Tasks • Readdress Tasks • Install Tasks • Migrate Tasks Click one of the tasks in the Task Queue to open the details for that task in the right top panel.

Setting	Description
Task status	

Setting	Description
	The top right portion of the Monitoring page shows the following information for a given task: • Status • Start time • Task data (for example: cluster data) To see details about the task, click on the View Log link. The following are the possible statuses for tasks: • Successful—Indicates that the task has finished without errors. • Started—Indicates that the task is currently running. • Scheduled—Indicates that the task has been scheduled, but has not yet started. • Manual Start—Indicates that the task is waiting to be started (user created the task with the "Start Task Manually" option). • Canceled—Indicates that the user chose not to run the task. • Paused—Indicates that the task is in a paused state waiting for feedback. • Paused due To Error—Indicates that the task is in a paused state due to an error in the system. • Failed—Indicates that the task has stopped because of an error. • Failed to Schedule—Indicates that the task was not scheduled, due to an error that occurred. • Failed to Cancel—Indicates that the user tried unsuccessfully to cancel the task. This typically happens when the task is in a final state (no actions are left to cancel). • Canceling—Indicates that the user canceled the task, but the task is in a state that will take a long time to cancel. The task may be in this state for an hour or more if the task being canceled is an installation or migration task (during the install-new-server phase). Possible messages and actions in a **Successful Status** state: • Task completed successfully • Delete—Deletes the task data permanently Possible actions in a **Started** state: • Cancel—Cancels the selected task • Delete—Deletes the selected task permanently Possible actions in a **Scheduled** state:

Setting	Description
	• Cancel—Cancels the selected task • Delete—Deletes the selected task permanently Possible actions in a **Waiting for Manual Start** state: • Start—Starts the task (You will see this button only if the Manual Start option was chosen when the task was created) • Delete—Deletes the selected task permanently Possible actions in a **Paused** state (a task enters this state if the user set up the task to pause at this step): • Resume—Task will continue at the next step • Cancel—Cancels the selected task • Delete—Deletes the selected task permanently Possible actions in a **Paused Due To Errors** state (a task will enter this state, because the system detected an error at this step): • Resume—Task will continue at the next step. (Before resuming, user should look at the error in the view log and correct the problem that caused the error, or else the task will fail.) If the error message says "Failed due to validation," the task will revalidate and start from the first step when you click Resume. Otherwise, the task will start from the next step. • Cancel—Cancels the selected task • Delete—Deletes the selected task permanently Possible action in a **Failed Status** state: • Delete—Deletes the selected task permanently
Start Task button	Starts task running for Scheduled tasks
Edit button	Opens Edit dialog for Scheduled tasks
Pause button	Pauses Running tasks (at next step)
Resume button	Resumes task at next step for Paused and Paused (Error) tasks
Cancel button	Cancels Scheduled, Running, Paused, and Paused (Error) tasks
Delete button	Deletes Scheduled, Canceled, Successful, and Failed tasks

Setting	Description
Task Summary	The Task Summary section contains the following information for a task: • Source Cluster • Destination Cluster • Unified Communications Manager Upgrade File • Unified Presence Upgrade File

Tasks View Elements

Upgrade View

Setting	Description
Scheduled Tasks and History table	
Status	Provides information about the upgrade task: • Successful—Indicates that the task has finished without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task has not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error
Start Time	Specifies the start time of the upgrade task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the name of the upgraded cluster
Notes	Note added during the Review portion of the Add Upgrade Task wizard

Setting	Description
Actions	

Setting	Description
	Allows you to perform the following for a particular upgrade task **Note** Depending on the state of the task, only some of these actions may be allowed (for example, an upgrade task that is completed cannot be canceled). • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all nodes are available and the iso to be used for upgrade is present. ◦ Edit—Shows the Edit Upgrade Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Use this button to restart task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action. **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—This causes the task to restart and retry the last failed task action. ◦ Resume—This causes the task to start at the next step (after the failed step). ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task

Setting	Description
	• Successful status: ◦ View Details—Navigates to the monitoring page showing all the tasks available. ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter upgrade tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—To show the tasks that are paused due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window.
Delete	Click the checkbox next to the task and click the Delete button at the top of the table. This action is applicable to tasks in the Failed, Successful, Scheduled and, Paused state.
Add Upgrade Task button	Opens the Add Upgrade Task wizard. **Note** You can also open the Add Upgrade Task wizard selecting Edit in the Actions column for a particular upgrade task.
Add Upgrade Task wizard window For information about how to Add an Upgrade Task, see “Create an Upgrade Task”.	

Setting	Description
Choose Cluster page	From the Choose Cluster page, select the cluster and product from the drop-down lists (All products is the default option for Products). Once you have selected the cluster, the list of nodes appears in the Cluster Nodes table.
Choose Upgrade File page	From the Choose Upgrade File page, select the upgrade file for each product being upgraded. You will have the option of selecting files only for the product type you selected on the Choose Cluster page.
Set Start Time and Upgrade Options page	From the Set Start Time and Upgrade Options page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting the task to begin immediately upon completion of the wizard. You also have the option of automatically switching to a new version following a successful upgrade.
Specify Run Sequence page	From the Specify Run Sequence, specify the sequence in which the upgrade will be processed on the servers. You change the sequence of steps by clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. Select the **Use Last Configured Run Sequence** box if you want to reuse the previous sequence. By default, each node is sequenced into its own step.
Review page	The Review page provides a summary of the options you have selected in the previous steps. The nodes listed in the Nodes field are view-only—you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Upgrade Task, on page 47

Switch Versions View

Setting	Description
Scheduled Tasks and History table	

Setting	Description
Status	Provides information about the switch version task: • Successful—Indicates that the task has finished without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task has not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error
Start Time	Specifies the start time of the switch version task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the switch version cluster
Notes	Notes that were added during the Review portion of the Add Switch Version wizard

Setting	Description
Actions	

Setting	Description
	The following are the status and the corresponding actions: • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all nodes are available and that none of the specified new addresses are reachable ◦ Edit—Shows the Edit Switch Version Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Restarts task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—This causes the task to restart and retry the last failed task action ◦ Resume—This causes the task to start at the next step (after the failed step) ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task • Successful status:

Setting	Description
	◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter switch version tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—To show the tasks that are paused due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window
Delete	Check the check box next to the task and click the Delete button at the top of the table. You can also click Delete under the Actions column for the task you wish to delete
Add Switch Versions Task button	Opens the Switch Versions Task wizard. **Note** You can also open the Switch Versions Task wizard by selecting Edit in the Actions column for a particular switch version task.
Add Switch Versions Task window For information about how to add a switch version task, see “Create a Switch Versions Task”.	

Setting	Description
Choose Cluster page	From the Choose Cluster page, select the cluster from the drop-down list. After you select the cluster, you must select the product versions (installed on the publisher) from the drop-down lists. If there is more than one product in the cluster, you have the option of not switching versions for one or more products. As long as one valid version is selected, you may proceed
Set Start Time page	From the Set Start Time page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting it to begin immediately upon completion of the wizard.
Set Run Sequence page	From the Specify Run Sequence, specify the sequence in which the version switch is processed on the servers. The sequence of the steps is changed by clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. Check the **Use Last Configured Run Sequence** check box if you want to reuse the previous sequence. By default, each node is sequenced into its own step. The Revert to Default button returns the steps to this original state.
Review page	The Review page provides a summary of the options you selected in the previous steps. The nodes listed in the Nodes field are view-only; you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Switch Versions Task, on page 50

Server Restart View

Setting	Description
Scheduled Tasks and History table	

Setting	Description
Status	Provides information about the server restart task: • Successful—Indicates that the task is complete without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task is not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error
Start Time	Specifies the start time of the server restart task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the server restart cluster
Notes	Notes that were added during the Review portion of the Add Restart Task wizard

Setting	Description
Actions	

Setting	Description
	The following are the status and the corresponding actions: • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all nodes are available and that none of the specified new addresses are reachable. ◦ Edit—Shows the Edit Upgrade Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Edit—Shows the Edit Server Restart Task window. Allows you to edit the selected task ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Restarts task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—This causes the task to restart and retry the last failed task action. ◦ Resume—This causes the task to start at the next step (after the failed step). ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task

Setting	Description
	• Successful status: ◦ View Details—Navigates to the monitoring page showing all the tasks available. ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter restart tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window.
Delete	Click the checkbox next to the task and click the Delete button at the top of the table. You can also click Delete under the Actions column for the task you wish to delete.
Add Server Restart Task button	Opens the Add Server Restart Task wizard. **Note** You can also open the Add Server Restart Task wizard by selecting Edit in the Actions column for a particular server restart task.
Add Server Restart Task window For information about how to add a server restart task, see “Create a Restart Task”.	

Setting	Description
Choose Cluster page	From the Choose Cluster page, select the cluster from the drop-down list. After you select the cluster, you will see that the nodes listed in the Cluster Nodes table change accordingly. Select the servers to be restarted.
Set Start Time page	From the Set Start Time page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting the task to begin immediately upon completion of the wizard.
Set Run Sequence page	From the Set Run Sequence page, specify the sequence in which the restart is processed on the servers. You can change the sequence of steps by clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. Check the **Use Last Configured Run Sequence** check box if you want to reuse the previous sequence. By default, each node is sequenced into its own step. The Revert to Default button returns the steps to this original state.
Review page	The Review page provides a summary of the options you have selected in the previous steps. The nodes listed in the Nodes field are view-only; you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Server Restart Task, on page 53

Readdress View

Setting	Description
Scheduled Tasks and History table	

Setting	Description
Status	Provides information about the readdress task: • Successful—Indicates that the task has finished without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task has not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error
Start Time	Specifies the start time of the readdress task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the readdress cluster
Notes	Note that were added during the Review portion of the Add Readdress Task wizard

Setting	Description
Actions	

Setting	Description
	The following are the status and the corresponding actions: • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all nodes are available and that none of the specified new addresses are reachable. ◦ Edit—Shows the Edit Readdress Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Edit—Shows the Edit Upgrade Task window. Allows you to edit the selected task ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Restarts task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—This causes the task to restart and retry the last failed task action. ◦ Resume—This causes the task to start at the next step (after the failed step). ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task

Setting	Description
	• Successful status: ◦ View Details—Navigates to the monitoring page showing all the tasks available. ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter readdress tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—To show the tasks that are paused due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window.
Delete	Check the check box next to the task and click the Delete button at the top of the table. You can also click Delete under the Actions column for the task you wish to delete.
Add Readdress Task button	Opens the Add Readdress Task wizard. **Note** You can also open the Add Readdress Task wizard by selecting Edit in the Actions column for a particular readress task.
Add Readdress Task window For information about how to Add a Readdress Task, see “Create a Readdress Task”.	

Setting	Description
Choose Cluster page	From the Choose Cluster page, select the cluster from the drop-down list. Click View Nodes to the nodes associated with this cluster. The View UC Cluster Nodes dialog box opens, listing the nodes in a table that identifies the following: • Hostname • IP Address • Product • Role The View UC Cluster Nodes dialog box is not editable. Click Close to return to the Choose Cluster page.
Enter New Hostnames/IP Addresses page	From the Enter New Hostnames/IP Addresses page, click Edit under the Actions column to open the Edit Hostname/IP Address dialog box. This dialog box allows you to enter a new hostname or IP address for the cluster nodes to be readdressed. You have the option of using DHCP or a static IP address.
Set Start Time page	From the Set Start Time page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting the task to begin immediately upon completion of the wizard. You can use this page to also enable the re-address option. Check the **Pause before network verification substeps to allow external changes** check box if you wish to introduce a pause between the re-address and the network change verification substeps upon changing the subnet or gateway. During this pause, you can make the necessary network changes to the virtual machine configuration, such as VLAN. **Note** After you make the changes, resume the task to complete the verification.
Set Run Sequence page	From the Set Run Sequence page, specify the sequence in which the readdress is processed on the servers. The sequence of the steps is changed by clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. Check the **Use Last Configured Run Sequence** check box if you want to reuse the previous sequence. By default, each node is sequenced into its own step. The Revert to Default button returns the steps to this original state.
Review page	The Review page provides a summary of the options you have selected in the previous steps. The nodes listed in the Nodes field are view-only; you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Readdress Task, on page 55

Install View

Setting	Description
Scheduled Tasks and History table	
Status	Provides information about the install task: • Successful—Indicates that the task has finished without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task has not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error
Start Time	Specifies the start time of the install task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the install cluster
Notes	Notes that were added during the Review portion of the Add Install Task wizard

Setting	Description
Actions	

Setting	Description
	The following are the status and the corresponding actions: • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all the ESXi host is present, the VMs are in the correct state, and the .iso file to be used in the install is present. ◦ Edit—Shows the Edit Upgrade Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Restarts task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—Retry the last failed step. This button causes the task to retry the last step that failed, and restart the task. ◦ Resume—Resumes the task at the next step. Use this option only if the failed step is non-essential, or if you have manually performed that step ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task • Successful status:

Setting	Description
	◦ View Details—Navigates to the monitoring page showing all the tasks available. ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter install tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—To show the tasks that are paused due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window.
Delete	Click the checkbox next to the task and click the Delete button at the top of the table. You can also click Delete under the Actions column for the task you wish to delete.
Add Install Task button	Opens the Add Installation Task wizard. **Note** You can also open the Add Installation Task wizard by selecting Edit in the Actions column for a particular install task.
Add Installation Task window For information about how to add an installation task, see “Create an Install Task”.	
Choose Installation Cluster page	From the Choose Cluster page, select the cluster from the drop-down list. After you select the cluster, you will see that the nodes listed in the Installation Cluster Nodes table change accordingly.

Setting	Description
Choose Installation Files page	From the Choose Installation Files page, select the installation images to be installed on the staging cluster. The ISO images must be uploaded to the /install directory on the system sftp server for Cisco Prime Collaboration Deployment.
Set Start Time page	From the Set Start Time page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting the task to begin immediately upon completion of the wizard.
Specify Installation Sequence page	From the Specify Installation Sequence page, specify the sequence in which the installation is processed on the servers. You can change the sequence of steps by clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. By default, each node is sequenced into its own step.
Review page	The Review page provides a summary of the options you have selected in the previous steps. The nodes listed in the Nodes field are view-only; you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Install Task, on page 57

Migrate View

Setting	Description
Scheduled Tasks and History table	
Status	Provides information about the migrate task: • Successful—Indicates that the task has finished without errors • Running—Indicates that the task is currently running • Scheduled—Indicates that the task has not yet started • Canceled—Indicates that the user has chosen not to run task • Paused—Indicates that the task is in a paused state waiting for feedback • Paused due To Error—Indicates that the task is in a paused state due to an error in the system • Failed—Indicates that the task has stopped due to error

Setting	Description
Start Time	Specifies the start time of the migrate task
Last Status Report Time	Specifies the time at which the action was completed. The completed action may be a success or failure.
Cluster	Specifies the cluster being migrated.
Notes	Notes that were added during the Review portion of the Add Migration Task wizard

Setting	Description
Actions	

Setting	Description
	The following are the status and the corresponding actions: • Scheduled status: ◦ Run Validation Test—Runs a validation test to ensure that all nodes are available and that none of the specified new addresses are reachable. It also checks that the ESXi hosts that the VMs reside on are mounted. It also verifies that the iso file to be used is present. ◦ Edit—Shows the Edit Upgrade Task window. Allows you to edit the selected task ◦ Cancel Task—Cancels the selected task ◦ Delete—Deletes the selected task permanently • Canceled status: ◦ Delete—Deletes the selected task permanently • Started status: ◦ Cancel Task—Cancels the selected task • Paused status: ◦ Resume—Restarts task at the next step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Start Task—Start task is present if the task is started manually. Time is not selected for this action **Note** Start Task is applicable only if you select **Start task manually** option in the **Set Start Time** panel. When you select the task manually, the resume option is unavailable in the monitoring page. ◦ Cancel Task—Cancels the selected task • Paused due to Error: ◦ Retry—Retry the last failed step. This button causes the task to retry the last step that failed, and restart the task. ◦ Resume—Resumes the task at the next step. Use this option only if the failed step is non-essential, or if you have manually performed that step. ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Cancel Task—Cancels the selected task

Setting	Description
	• Successful status: ◦ View Details—Navigates to the monitoring page showing all the tasks available. ◦ Delete—Deletes the selected task permanently • Failed status: ◦ View Details—Navigates to the monitoring page showing all the tasks available ◦ Delete—Deletes the selected task permanently
Show	Allows you to filter migration tasks by status, by selecting one of the following options from the drop-down list: • Quick Filter—To filter the tasks based on the status • All—To show all the tasks available • Scheduled—To show the tasks that are scheduled • Canceled—To show the tasks that are canceled • Running—To show the tasks that are started • Paused—To show the tasks that are paused • Paused due To Error—To show the tasks that are paused due to an error in the system • Successful—To show the tasks that are successful • Failed—To show the tasks that failed
Filter	Select a status and click Filter to set a search rule at the bottom of the search window.
Delete	Check the check box next to the task and click the Delete button at the top of the table. You can also click Delete under the Actions column for the task you wish to delete.
Add Migration Task button	Opens the Add Migration Task wizard. **Note** You can also open the Add Migration Task wizard by selecting Edit in the Actions column for a particular migrate task.
Add Migration Task window For information about how to add a migration task, see “Add Migration Task”.	

Setting	Description
Choose Source and Destination Clusters page	From the Choose Source and Destination Clusters page, select the source UC cluster from the drop-down list. After you select the source cluster, you select the destination cluster from the drop-down list and the nodes from the Node Mapping from Source to Destination Cluster table.
Choose Upgrade Files page	From the Choose Upgrade File page, select the upgrade file for each product being upgraded. You will only have the option of selecting files for the product type you selected on the Choose Cluster page.
Set Start Time page	From the Set Start Time page, select a start time for the task. **Note** The time specified is based on the Cisco Prime Collaboration Deployment server time, not the time zone of the selected cluster. You have the option of setting the start time for a specific time, starting the task manually, or setting the task to begin immediately upon completion of the wizard.
Specify Migration Procedure page	From the Specify Migration Procedure page, specify the sequence in which the migration is processed on the servers. You can change the sequence of the stepsby clicking the up and down arrows of a particular step. You can also add or delete a step, or edit an existing step. By default, each node is sequenced into its own step. The Revert to Default button returns the steps to this original state.
Review page	The Review page provides a summary of the options you have selected in the previous steps. The nodes listed in the Nodes field are view-only; you cannot select them. You can add notes to the Notes field for future reference.

Related Topics

Migration Task, on page 36

Inventory View Elements

Clusters

Setting	Description
Clusters table	
Cluster Name	Shows the available clusters
Product and Version	Shows the product for which the cluster is added along with its version

Setting	Description
Nodes	Shows the number of nodes associated with the cluster
Cluster Type	Shows the cluster type, such as Discovered, New install, or Migration
Discovery Status	Shows the discovery status of a cluster. This field shows one of the following discovery statuses: • Contacting • Discovering • Successful • Node Unreachable • Timeout • Internal Error
Actions	Includes the following options: • **Edit—**Edit an added new node that has not yet been installed • **Delete—**Delete an added new node that has not yet been installed
Show	Allows you to filter cluster tasks by status, by selecting one of the following options from the drop-down list: • All—To show all the available clusters • Discovered—To show the clusters that are scheduled • New Install—To show the cluster that newly installed • Migration—To show the clusters that are migrated
Filter	Select a status and click **Filter** to set a search rule at the bottom of the search window.
Discover Cluster button	Click this button so that Cisco Prime Collaboration Deployment communicates with the servers that are already running Unified Communications applications and adds that cluster information into the Cisco Prime Collaboration Deployment inventory
Define Migration Destination Cluster For information on how to create a migration cluster, see Create a Migration Cluster, on page 32.	

Setting	Description

Specify Clusters page	Enter details for the following fields to configure a destination cluster for a migration task:
	• **Source Cluster—**From the drop-down list, select a source UC cluster.
	• **View Nodes—**Click this link to view the available cluster nodes.
	• **Active Versions—**Shows the active versions of the source UC cluster.
	• **Destination Cluster Nickname—**Enter a nickname for the destination cluster.
	• **Destination Network Settings—**Choose one of the following options:
	  • **Use the source node network settings for all destination nodes—**Choose this option to retain the default network options.
	  • **Enter new network settings for one or more destination nodes—**Choose this option to modify the default network settings or enter new network options.
	  Note If you select the **Use the source node network settings for all destination nodes** option, same IP address appears for both the source node **NAT IP** and **Dest NAT IP** columns on the **Assign Destination Cluster Nodes** window. If you select the **Enter new network settings for one or more destination nodes** option, only source hostname appears and not the destination hostname on the **Assign Destination Cluster Nodes** window.

Assign Destination Cluster Nodes page	• **Source Cluster—**Displays the name of the source cluster. • **Destination Cluster—**Displays the name of the destination cluster. • **Assign Destination Cluster Nodes—**Click this button to associate destination virtual machines with nodes in the source cluster. **Note** If DHCP is in use on your source node, the destination node is also configured to use DHCP, and you will have no option to change your network settings in this wizard.

Setting	Description
Configure NTP/SMTP Settings	Enter details for the following sections to configure NTP and SMTP to the migration nodes when the migration task is run: **Network Time Protocol (NTP) Configuration** window—Enter IP address of at least one of the following fields: • **NTP Server 1** • **NTP Server 2** • **NTP Server 3** • **NTP Server 4** • **NTP Server 5** (Optional) **Simple Mail Transfer Protocol (SMTP) Configuration** window • **SMTP Server—**Enter IP address of the SMTP server.
Define DNS Settings	(Optional) From the available hosts added along with the functions, check a node to configure DNS setting for the migration cluster nodes and click **Assign DNS Settings**
Discover Cluster window For information on how to Discover a Cluster, see Discover a Cluster, on page 29.	
Cluster Access page	Enter details in the following fields: • **Choose a Nickname for this Cluster—**Enter a nick name for the cluster. • **Hostname/IP Address of Cluster Publisher—**Enter either the host name or the IP address for the publisher node of the cluster. • **OS Admin Username—**Enter the OS administrator user name. • **OS Admin Password—**Enter the password for the OS administrator. • **Enable NAT—**Check this check box to enable NAT for the cluster. **Note** When you check the **Enable NAT** check box, the **NAT IP** column appears on the Cluster Discovery Progress page.

Setting	Description

Cluster Discovery Progress page	This page displays the status of cluster discovery in the following fields:
	• **Cluster Name—**Shows the cluster name along with the status message of the cluster discovery.
	• **Hostname—**Shows the host name.
	• **Contact Status—**Shows the one of the following statuses for cluster discovery:
	  • Contacting
	  • Discovering
	  • Successful
	  • Node Unreachable
	  • Timeout
	  • Internal Error
	• **Product—**Shows the product of the cluster.
	• **Active version—**Shows the version currently in use.
	• **Inactive version—**Shows the version that is currently not in use.
	• **NAT IP—**This column appears only if you check the **Enable NAT** check box on the Cluster Access page.
	• **Hardware—**Shows the hardware associated to the cluster.

Cluster Role Assignment page	
Define New UC Cluster window For information on how to install a new cluster, see Add New Cluster for Fresh Install, on page 34. After you click this button, a wizard appears that guides you to the installation process of a new UC cluster.	
Specify Cluster Name window	**Choose the Nickname for this cluster—**Enter the cluster name

Setting	Description

Add Virtual Machines window	Enter details in the following fields:
	• **Add Node—**Check one or more functions for adding a node from the available check boxes.
	• **Notes—**(Optional) Add a nodes for the selected cluster.
	• **Virtual Machines—**Add a node from the available virtual machines.
	Note The available VMs are sorted by name and by host. The details of virtual machines, such as VM Name, ESXi Host, and Power State, appear in this window.
	• **Show—**Allows you to filter virtual machine by status, by selecting options from the drop-down list.
	• **Network—**Select one of the following options:
	  • **Static IP address—**Enter the details for hostname, IP Address, Subnet Mask, Gateway, and NAT IP fields.
	  • **Use DHCP with Reservations—**Enter the IP address that you have a reservation for on your DHCP server (associated with the MAC address for that VM) in addition to the hostname.
	• **Products and Functions—**From the drop-down list, select a product. In the Functions section, check the appropriate function check boxes for your VM.
	Note • Check the **Publisher** check box for at least one node in the cluster that you have defined for each application type.
	• (Optional) Add a note about the functions that you have assigned in the **Notes** field below the **Publisher** field.
	• Virtual Machines section—Choose a VM for the selected node.

Setting	Description
Configure Cluster Wide Settings window	Enter details for the fields of the following sections: **OS Administration Credentials** • **Username—**Enter user name of the OS administrator. • **Password—**Enter password of the user name. • **Confirm Password—**Re-enter the same password that you entered in the **Password** field. **Application Credentials** • **Username—**Enter user name of the application user. • **Password—**Enter password of the user name. • **Confirm Password—**Re-enter the same password that you entered in the **Password** field. **Security Password** • **Password—**Enter the security password for the cluster. • **Confirm Password—**Re-enter the same password that you entered in the **Password** field. **SMTP Settings** (Optional) • **SMTP Server—**Enter the IP address of the SMTP server. **Certificate Information** • **Organization—**Enter the name of the organization of which the certificate is being used. • **Unit—**Enter the number of certificates being used. • **Location—**Enter the location where the certificate is being used. • **State—**Enter the state where the certificate is being used. • **Country—**From the drop-down list, select the country where the certificate is being used.
Configure DNS Settings window	(Optional) From the available hosts added along with the functions, check a node to configure DNS setting for a node and click **Assign DNS Settings**.

Setting	Description
Configure NTP Settings	To configure the Network Time Protocol, enter details of at least one NTP server in the following fields. If you are not using DNS, NTP server must be an IP address. If you are using DNS, NTP server can be an FQDN. • **NTP Server 1** • **NTP Server 2** • **NTP Server 3** • **NTP Server 4** • **NTP Server 5** **Note** It is recommended that you define at least IP addresses of two NTP servers
Configure NIC Settings	(Optional) Enter details for the following fields: • Hostname, Functions, and MTU size column—From the available servers, check the check box for a server. • **MTU Size—**Enter an MTU size between 552 and 1500 and click **Apply to Selected**. • **Apply to Selected—**Click this button to apply the MTU size for the selected host. • **Apply Default MTU—**Click this button to apply the default value of MTU size for the selected host.
Configure Time Zones window	Enter details for the following fields to specify the time zone for each cluster node: • **Region—**From the drop-down list, select the region for the cluster node. • **Time Zone—**From the drop-down list, select the time zone of the selected region. • **Apply to Selected—**Click this button to apply the time zone changes for each cluster node.

ESXi Hosts View

Setting	Description
ESXi Hosts table	
Hostname	Shows the ESXi host name.

Setting	Description
IP Address	Shows the IP address of the ESXi host.
Description	Shows the description, if any, of the ESXi host.
Actions	Includes the following options: • **Edit—**Click this link to edit the ESXi host details. • **Delete—**Click this link to delete the ESXi host from the database.
Add ESXi Host	Click this button to add an ESXi host in the database.
Add ESXi Host window	
Hostname/IP Address	Enter the host name of the IP address of the ESXi host.
Username	Enter the user name.
Password	Enter the password for the user.
Description	(Optional) Enter the description for the ESXi host.

SFTP Servers and Datastore

Setting	Description
SFTP Servers/Datastore section The Cisco Prime Collaboration Deployment server serves as a local SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP) server that stores the ISO and COP files to be used by upgrade, fresh, install, and migrate tasks. For more information on SFTP Datastore, see SFTP Servers and Datastore, on page 121.	
Delete	Click this button to delete the selected SFTP server from the datastore.
Add Server	Click this button to add the selected SFTP server to the datastore.
Server IP	Shows the IP addresses of the available SFTP servers in the datastore.
Server Description	Shows the description added for the available SFTP servers.
Database Directory	Shows the directory path of the SFTP servers.
Status	Shows the status of the SFTP server. For example, Connected and Local.

Setting	Description
Actions	Includes the following options: • **Edit—**Click this link to edit the SFTP server details. • **Delete—**Click this link to delete the selected SFTP server from the datastore.
SFTP/Datastore Files section	
Delete	Click this button to delete the ISO and COP files of the selected SFTP server from the datastore.
Filename	Shows the available ISO and COP files of the SFTP servers.
Server IP	Shows the IP address of the SFTP servers.
Server Description	Shows the description added for the available SFTP servers.
Directory	Shows the directory name where the SFTP files of the SFTP servers are stored.
File Type	Shows the type of file, such as upgrade file and fresh install.
Copied On (local)	Shows the data, time, and time zone when the SFTP file is copied to the datastore.

Administration View Elements

Email Notification View

Setting	Description
Notification Settings section For more information, see Email Notification, on page 65.	

Setting	Description
Notifications	Select one of the following options: • **Do not send email notification—**Choose this option if you do not wish to receive any email notification for errors or types of tasks. **Note** If you choose this option, all the fields of this section become non-editable. • **Errors only - Send email only when there is an error—**Choose this option if you wish to receive email notifications for task event errors in the following states: • Failed to Schedule • Failed • Failed to cancel • Paused on error • **Standard - Send email when tasks start, pause, finish, or when there is an error—**Choose this option if you wish to receive email notifications when a task enters any of the following states: • Scheduled • Failed to Schedule • Started • Successful • Failed • Canceled • Canceling • Failed to Cancel • Paused on Error • Paused • Paused – Required
Email Recipients	Enter the email address of one or multiple recipients. **Note** Separate multiple email addresses with a comma.
Use TLS	Check this check box so that Transport Layer Security (TLS) protocol ensures privacy or prevent tampering with the email between the application and the email recipients.
Mail server credentials section	

Setting	Description
Username	Enter the user name of the mail server.
Password	Enter the password to log in to the mail server.
Server Settings section	
SMTP Server	Enter the IP address of the SMTP server.
Port	Enter the number of ports for the SMTP server.
Save	Click this button to save the changes you have made in this page.
Reset	Click this button to set the default values on this page.
Send Test Email	Click this button to send a test email to one or more recipients for the errors only and standard options.

NAT Settings

Setting	Description
PCD NAT Settings For more information on network address translation, see Network Address Translation Support, on page 23.	
Hostname	Shows the host name of the server.
Private IP	Shows the IP address of the server that is in the private network.
NAT IP	Enter the NAT IP address.
Save	The NAT IP address is saved as an entry in a configuration file on Cisco Prime Collaboration Deployment. This entry is used when the application nodes try to contact Cisco Prime Collaboration Deployment.
Reset	(Optional) The NAT IP address is reset to the earlier saved NAT IP address.

Disk Space Warning Level

Setting	Description
Disk Space Warning Level Configuration For details, see Disk Space Warning Level, on page 71.	
Total Disk Space (GB)	Shows the total disk space on the server.
Available Disk Space (GB)	Shows the available disk space for use on the server.
Warning Level Disk Space (GB)	Enter the disk space warning value. After entering this value, click the information link to check if the space value you entered is available for use on the server.
Save	Save the warning disk space value.
Reset	(Optional) Resets the page with the default values.

Audit Log Configuration

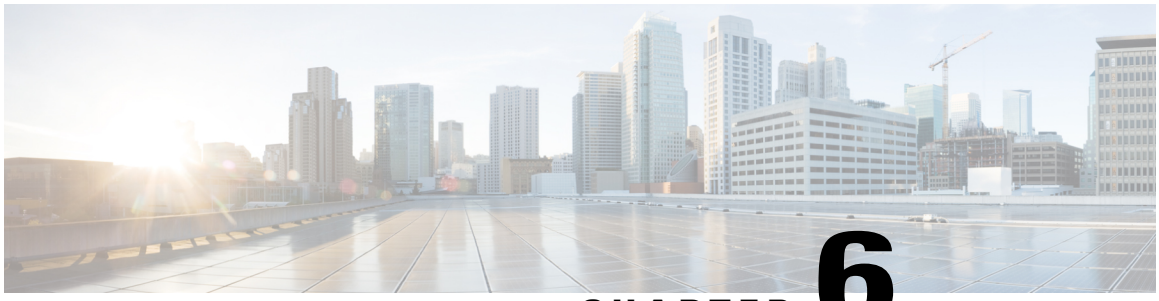
Setting	Description
Audit Level Settings section	
Application Audit Event Level	From the drop-down list, choose one of the following options: • **Info—**To view the audit event level as an information message. • **Warning—**To view the audit event level as a warning message. • **Debug—**To view the audit event level as a debug message. • **Error—**To view the audit event level as an error message.
Remote SysLog Settings section	
Remote Syslog Server Name / IP	Enter the name of remote syslog server or the IP address for the audit logs to be logged in to this remote server.
Local Audit Log Settings	

Setting	Description
Enable Local Audit Log	Check or uncheck this check box to enable or disable the local audit log. **Note** • When you check this field, the audit events are logged in the local server. When you uncheck this field, audit events are not logged in the local server. • When you check this field, the **Enable Log Rotation** field becomes active.
Enable Log Rotation	Check or uncheck this check box to enable or disable the log rotation. **Note** • You can configure this field if the **Enable Local Audit Log** field is enabled. • After you enable this field, you can configure the **Maximum No of Files**, **Maximum File Size(MB)**, and **Warning Threshold for Approaching Log Rotation Overwrite(%)** fields. When you uncheck the **Enable Local Audit Log** field, the default values of these fields are not applicable as they are not active.
Maximum No of Files	Enter an integer value for the **Maximum No of Files** field to configure the maximum number of files that can be created on the server. After you check the **Enable Log Rotation** field, you can configure the value for **Maximum No of Files** field. Once the number of files reaches the configured value, the log rotation process starts. In the log rotation process, all the log files are deleted and rewritten from the log file number 1. **Note** The value for this field must be in the range of 1 to 5000.
Maximum File Size(MB)	Enter a value for the **Maximum File Size (MB)** field to configure the maximum file size of each log that is created on the server. **Note** The value for this field must be in the range of 1 to 10.

Setting	Description
Warning Threshold for Approaching Log Rotation Overwrite(%)	Enter the warning threshold value for the **Warning Threshold for Approaching Log Rotation Overwrite(%)** field. After the configured warning threshold value is reached, an email notification is sent to users to take back up of the audit log files. These files are deleted or overwritten during log rotation. **Note** The value for this field must be in the range of 1 to 100. For details, see the Email notification topic in the *Cisco Prime Collaboration Deployment Administration Guide*.
Save	Click this button to save the changes you have made on this page.
Reset	Click this button to set the default values on this page.

Customized Logon Message Configuration

Setting	Description
Upload Customized Logon File	
Upload File	Click the **Browse** button to browse to the location of file that includes the customized sign-on message.
Require User Acknowledgment	Check or uncheck this check box to enable or disable user acknowledgment for the file that the user receives. If this field is enabled, users get an acknowledgment as an alert message on the Cisco Prime Collaboration Deployment sign-in page. This message appears after they sign out for the first time from the same web browser instance.
Upload File	Click this button to upload the file with the customized sign-on message to the server. After you upload the file, a popup appears showing the file upload status.
Delete	Click this button to delete the file with the customized sign-on message. After you delete the file, popup appears showing the file deletion status.



CHAPTER 6

Cisco Prime Collaboration Deployment Configuration and Administration

- Services, page 129
- Limitations and Restrictions, page 133

Services

After the installation of the Cisco Prime Collaboration Deployment platform, most services start automatically. You can configure services by setting service parameters for each service. If necessary, for example, for troubleshooting purposes, you may need to stop, start, or restart a service. You can perform these tasks by using the CLI on the Cisco Prime Collaboration Deployment platform.

Cisco Prime Collaboration Deployment Service

This service supports the Cisco Prime Collaboration Deployment application interface. This service must be active for the Cisco Prime Collaboration Deployment application to work correctly. It is active by default.

Performance and Monitoring Services

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on the Cisco Prime Collaboration Deployment platform by using configured thresholds and a polling interval.

Cisco RIS Data Collector

The Real-Time Information Server (RIS) maintains real-time information, such as critical alarms generated.

Cisco AMC Service

The Alert Manager and Collector (AMC) service allows you to retrieve real-time information that exists on the server.

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any configuration change to the Cisco Prime Collaboration Deployment platform by a user or as a result of the user action.

SOAP-Log Collection APIs Service

The Cisco SOAP-Log Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, Cisco application trace files.

SOAP-Performance Monitoring APIs Service

The Cisco SOAP-Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service and CPU usage.

Backup and Restore Services

Cisco DRF Master

The Cisco Disaster Recovery Framework (DRF) Master Agent service supports the DRF Master Agent, which works with the CLI to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which performs the work for the DRF Master Agent. Components register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent runs commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

SFTP

Cisco Prime Collaboration Deployment runs a Secure File Transfer Protocol (SFTP) server locally.

System Services

CDP

Cisco Delivery Protocol (CDP) advertises the voice application to other network management applications, so the network management application can perform network management tasks for the voice application.

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces. If you stop this service, you cannot collect or view traces on the Cisco Prime Collaboration Deployment platform.

For SysLog Viewer and trace and log collection, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces. If you stop this service, you cannot collect or view traces on the Cisco Prime Collaboration Deployment platform.

For SysLog Viewer and trace and log collection, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Tip If necessary, to reduce the initialization time, we recommend that you restart the Cisco Trace Collection Service before restarting the Cisco Trace Collection Servlet.

Platform Services

Cisco Tomcat

The Cisco Tomcat service supports the web server.

Cisco Tomcat Stats Servlet

The Cisco Tomcat Stats servlet collects the Tomcat statistics.

Platform Administrative Web Service

The Platform Administrative Web service is a SOAP API that can be activated on Cisco Unified Communications Manager, Cisco Unified Presence, IM and Presence Service, Cisco Unified Contact Center Express, or Cisco Unity Connection systems, to allow the Cisco Prime Collaboration Deployment server to upgrade the system.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to Simple Network Management Protocol (SNMP) requests.

Tip After you complete SNMP configuration in the CLI, you must restart the SNMP Master Agent service.

MIB2 Agent

The Management Information Base (MIB2) Agent service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables; for example, system and interfaces.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, and installed software base. This service implements the HOST-RESOURCES-MIB.

System Application Agent

This service provides SNMP access to the applications that are installed and running on the system. This service implements the SYSAPPL-MIB.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Prime Collaboration Deployment platform. This service implements the CISCO-CDP-MIB.

Cisco Syslog Agent

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date.

Working with Services

To start, stop, activate, or restart services or to configure service parameters for services on the Cisco Prime Collaboration Deployment platform, you must use the CLI. You can start, stop, activate, or refresh only one service at a time.

Note When a service is stopping, you cannot start it until after the service is stopped. Also, when a service is starting, you cannot stop it until after the service is started.

The following services are activated by default after you install the Cisco Prime Collaboration Deployment platform.

- Cisco AMC Service
- Cisco Audit Event Service
- Cisco CDP
- Cisco CDP Agent
- Cisco Certificate Expiry Monitor
- Cisco DRF Local
- Cisco DRF Master
- Cisco Log Partition Monitoring Tool
- Cisco Platform Manager Service
- Cisco RIS Data Collector
- Cisco Syslog Agent
- Cisco Tomcat
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Servlet
- Host Resources Agent

- MIB2 Agent
- SNMP Master Agent
- System Application Agent

The following services are stopped by default after you install the Cisco Prime Collaboration Deployment platform.

- Cisco Trace Collection Service
- SOAP-Log Collection APIs
- SOAP-Performance Monitoring APIs

Caution Some changes to service parameters may cause system failure. We recommend that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

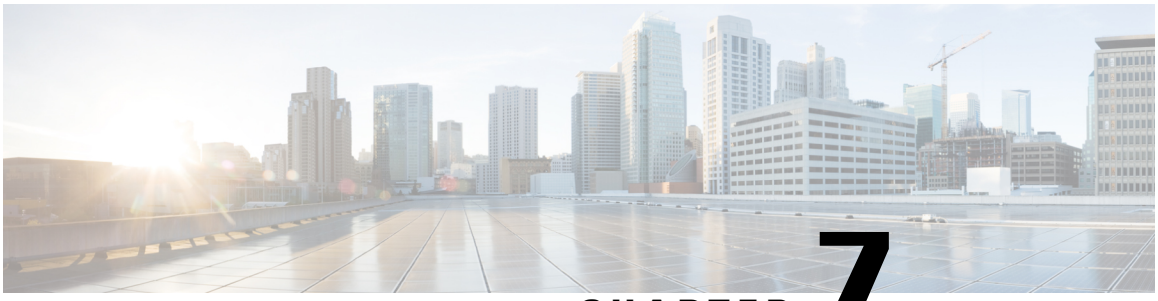
The following table shows the commands that you need to work with services on the Cisco Prime Collaboration Deployment platform.

Table 13: Service CLI Commands

Task	Command
Display a list of services and service status	**utils service list**
Activate a service	**utils service activate**
Stop a service	**utils service stop** *servicename*
Start a service	**utils service start** *servicename*
Restart a service	**utils service restart** *servicename*

Limitations and Restrictions

- Cisco Prime Collaboration Deployment is not a diagnostic tool. An error message appears on the task list page if a task fails; however, you should use your usual set of tools and procedures to diagnose and correct the problem.
- The SOAP services do not replace the existing OS Administration and CLI upgrade processes. You can still upgrade your servers by using the application GUIs or CLI commands. Cisco Prime Collaboration Deployment is another way to upgrade, restart, or switch versions on the application servers.
- No localization is available for Cisco Prime Collaboration Deployment. The localization is available in English only (including time and date formats).



CHAPTER 7

CLI Commands and Disaster Recovery System

- CLI Commands on Cisco Prime Collaboration Deployment, page 135

CLI Commands on Cisco Prime Collaboration Deployment

The main functions of Cisco Prime Collaboration Deployment (such as creating migration, upgrade, and other tasks) are supported through the Cisco Prime Collaboration Deployment GUI interface. You can use the GUI interface to create a specific task and schedule the time to perform the task. The GUI interface also reports the status of tasks.

For other operations, such as upgrading the software on the Cisco Prime Collaboration Deployment server and performing a DRS backup, use the Cisco Prime Collaboration Deployment CLI, which is similar to the CLI on Cisco Unified Communications Manager Release 10.x.

Use the CLI on Cisco Prime Collaboration Deployment to perform the following tasks:

- View or get log files
- Administer a DRS backup device, and perform a data backup or restore
- Upgrade the Cisco Prime Collaboration Deployment software
- Change the hostname, IP address, or password on the Cisco Prime Collaboration Deployment
- Perform diagnostic commands on the Cisco Prime Collaboration Deployment system

The most common CLI operations and commands are for viewing logs and performing DRS backups.

Getting Cisco Prime Collaboration Deployment Logs

When you troubleshoot problems on the Cisco Prime Collaboration Deployment server, it is often necessary to view the main application log.

CLI command: **file get activelog tomcat/logs/ucmap/log4j/***

The Cisco Prime Collaboration Deployment main application log contains the following information:

- Representational state transfer (REST) requests from the browser
- Simple Object Access Protocol (SOAP) requests to UC servers
- Database requests

- Scheduler events (scheduled, started, failed, and so on)
- Specific job events (tasks, task actions, and nodes)
- Exceptions and errors

DRS on Cisco Prime Collaboration Deployment

The Disaster Recovery System (DRS) can be administered and invoked from the Cisco Prime Collaboration Deployment CLI. DRS allows you to perform user-invoked data backups of the data on your Cisco Prime Collaboration Deployment (the server clusters you have discovered, and scheduled and completed tasks). You can also choose to set up regularly scheduled automatic backups. The DRS feature has the following functions:

- CLI commands for performing backup and restore tasks
- The ability to schedule backups ahead of time, or run backups manually immediately
- The ability to archive backups to a remote SFTP server

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup and restore.

Important While you restore your data, the hostname, server IP address, and Cisco Prime Collaboration Deployment software version on the machine to which you are restoring the data must be the same as they were on the server on which you performed the backup.

DRS CLI Commands

Below is a list of the CLI commands that you can use to configure and perform backup and restore operations through DRS.

- **utils disaster_recovery status <operation>** (An example of **operation** is Backup or Restore).
- **utils disaster_recovery device list**
- **utils disaster_recovery device add**
- **utils disaster_recovery device delete**
- **utils disaster_recovery schedule add**
- **utils disaster_recovery schedule delete**
- **utils disaster_recovery schedule enable**
- **utils disaster_recovery schedule disable**
- **utils disaster_recovery schedule list**
- **utils disaster_recovery backup —**Starts a manual backup by using the features that are configured in the DRS interface.
- **utils disaster_recovery restore —**Starts a restore, and requires parameters for backup location, filename, and features to restore.
- **utils disaster_recovery show_backupfiles—**Shows existing backup files.
- **utils disaster_recovery cancel_backup**

- **utils disaster_recovery show_registration**
- **utils disaster_recovery show_registration SERVER—**Shows the features that you need to back up. For example, if you want to back up Cisco Prime Collaboration Deployment, choose `PCD` from the feature list.

For more information, see the DRS documentation for Cisco Unified Communications Manager, at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Create a DRS Backup of the Server

Before You Begin

If you are using a location on your network to back up your Cisco Prime Collaboration Deployment, ensure the following points:

1. You must have access to an SFTP server to configure a network storage location. The Disaster Recovery system supports only SFTP servers that are configured with an IPv4 address or hostname/FQDN.
2. The account that you use to access the SFTP server must have write permission for the selected path.

You can also back up your Cisco Prime Collaboration Deployment to a local disk; however, this method is not recommended, because of the amount of space that is required on the Cisco Prime Collaboration Deployment disk to store the backup files.

Procedure

Step 1 Add the backup device.
Run the following command: **utils disaster_recovery device add network**

Example:
utils disaster_recovery device add network device1 /backupdir/pcdbk 10.94.155.76 adminname 2

Step 2 To verify that the device was set up correctly, run the following CLI command: **disaster_recovery device list**.

Step 3 Run a backup using the following command:
utils disaster_recovery backup network PCD device_name where device_name is the name of the backup device that was defined in Step 1.

Example:
utils disaster_recovery backup network PCD device1

Step 4 Check the status of the backup using the following CLI command:
utils disaster_recovery status backup.Use this command to see the status of your backup. The backup is complete when Percentage Complete is 100, and all components show “SUCCESS.”

Important Notes on Backup and Restore

Note When you restore your Cisco Prime Collaboration Deployment data, ensure that the Cisco Prime Collaboration Deployment software version that is installed on your server matches the version of the backup file that you want to restore.

Note When you perform a DRS restore operation to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present before you perform a restore operation.

Note We recommend that you perform a fresh installation of Cisco Prime Collaboration Deployment on your virtual machine before you restore the data.

Restore a Backup to Cisco Prime Collaboration Deployment

Note This procedure is optional.

Procedure

Step 1 Because a fresh install of the VM is recommended before the restore, you will need to add a backup device, so the system can retrieve the files from there. Configure the backup device by using the **utils disaster_recovery device add network** command.

Example:
utils disaster_recovery device add network device1 /backupdir/pcdbk 10.94.155.76 adminname 2
Specify the device from which you want to restore a backup file.

Step 2 List the backup files by using the following CLI command: **utils disaster_recovery show_backupfiles**

Example:
admin: utils disaster_recovery show_backupfiles device1
The **show_backupfiles command** shows which backups are available to be restored. Backups are named by date and the time the backup was performed.

Step 3 Start the restore operation by running the following CLI command: **utils disaster_recovery restore network**

Example:
admin:utils disaster_recovery restore network b7k-vmb031 2013-10-30-15-40-54 device1
When you are prompted to enter the features to restore, enter PCD.
Enter the comma separated features you wish to restore. Valid features for server B7K-VMB031 are PCD:PCD.

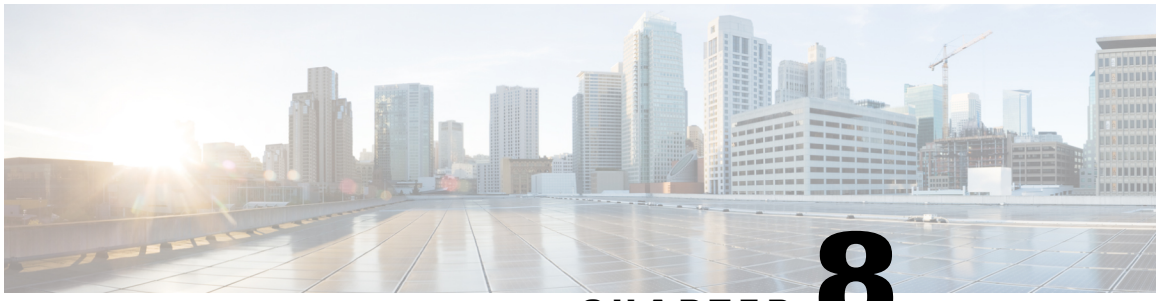
Step 4 Check the status of the restore by using the following CLI command: **utils disaster_recovery status restore**. While the restore process is running, you can check the status of the current restore job.

Do not administer any data on the Cisco Prime Collaboration Deployment server until the command shows as one hundred percent complete. This can take several minutes, depending on the amount of data that is being restored.

What to Do Next

After you restore your data, perform a system restart on the Cisco Prime Collaboration Deployment server to initialize the database.

The Cisco Prime Collaboration Deployment server will lose contact with ESXi hosts during the reinstallation. You may have to add ESXi hosts back into Cisco Prime Collaboration Deployment after a restore operation.



CHAPTER 8

CLI Commands for EnhancedSecurityMode and FIPS Mode

- CLI Commands for EnhancedSecurityMode, page 141
- CLI Commands for FIPS Mode, page 142
- User Account and Sign-in Attempts on CLI and Interface, page 144
- Configure Remote Audit Logging for Platform Logs, page 144
- Platform CLI Commands for Security in EnhancedSecurityMode, page 146

CLI Commands for EnhancedSecurityMode

Use the following CLI commands for EnhancedSecurityMode:

- **admin:utils EnhancedSecurityMode**
- **utils EnhancedSecurityMode disable**
- **utils EnhancedSecurityMode enable**
- **utils EnhancedSecurityMode status**

Configure EnhancedSecurityMode

An administrator can use this procedure on Cisco Prime Collaboration Deployment to configure EnhancedSecurityMode. When this mode is enabled, the following system enhancements are updated automatically:

- Stricter credential policy for password changes is implemented
- TCP becomes the default protocol for remote audit logging
- FIPS mode is enabled

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils EnhancedSecurityMode status** command to confirm whether Enhanced Security Mode is enabled.

Step 3 To configure Enhanced Security Mode, run one of the following commands on a node:

- To enable this mode, run the **utils EnhancedSecurityMode enable** command.
- To disable this mode, run the **utils EnhancedSecurityMode disable** command.

CLI Commands for FIPS Mode

Use the following CLI commands for FIPS mode on Cisco Prime Collaboration Deployment:

- **utils fips enable—**Enable FIPS mode. For details, see the Enable FIPS Mode, on page 142 procedure.
- **utils fips disable—**Disable FIPS mode. For details, see the Disable FIPS Mode, on page 143 procedure.
- **utils fips status—**Provide the details whether FIPS mode is enabled or disabled on a server.

Note The disaster recovery system CLI commands are supported in FIPS mode. For details on these commands, see the CLI Commands and Disaster Recovery System chapter of the *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Enable FIPS Mode

You can enable the FIPS mode through CLI.

Caution Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Procedure

Step 1 Start a CLI session.

Step 2 In the CLI, enter **utils fips enable**
The following prompts appear:

```
admin:utils fips enable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the
above
components will need to be re-uploaded.
******************************************************************************
This will change the system to FIPS mode and will reboot.
******************************************************************************

Do you want to continue (yes/no) ?
```

Step 3 Enter **yes**.
The following message appears:

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
*******************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
*******************************************************
The system will reboot in a few minutes.
```

Cisco Prime Collaboration Deployment reboots automatically.

Disable FIPS Mode

You can disable FIPS mode through the CLI using the following procedure:

Procedure

Step 1 Start a CLI Session.

Step 2 In the CLI, enter **utils fips disable**
The following prompts appear:

```
admin:utils fips disable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the
above
components will need to be re-uploaded.
******************************************************************************
```

```
This will change the system to NON-FIPS mode and will reboot.
********************************************************************************

Do you want to continue (yes/no) ?
```

Step 3 Enter **yes**.
Cisco Prime Collaboration Deployment reboots and is restored to non-FIPS mode.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

User Account and Sign-in Attempts on CLI and Interface

Following table lists the scenarios when a user signs in to the Cisco Prime Collaboration Deployment application or CLI and the result of sign in attempts:

User Sign-in Scenario	Result of Sign-in Attempt
Sign-in with the valid credentials	Sign-in is successful and the application home page is accessible
Sign-in with invalid credentials	Sign-in fails
Sign-in after exceeded number of attempts on the application	Account is locked after three consecutive unsuccessful attempts
Sign-in after exceeded number of attempts on the CLI	CLI sign-in fails due to locked account even though the user types in the correct password
Sign-in to the application after the lockout period expires	After 5 minutes of lockout period, the application is available for you to sign-in
Sign-in to CLI after the lockout period expires	After 5 minutes of lockout period expiry, the account gets unlocked and you can sign-in to the CLI
Sign-in to the application when the account is locked due to inactivity	Account gets locked due to inactivity of the session
Sign-in to the application after account lockout, which is caused due to inactivity, is resolved	Sign-in is successful

Configure Remote Audit Logging for Platform Logs

Complete the following tasks to add remote audit logging support for platform audit logs, remote support logs, and csv files. For these types of logs, the FileBeat client and logstash server are used.

Before You Begin

Ensure that you have set up an external logstash server.

Procedure

Step 1 Configure the FileBeat client with the external logstash server details, such as IP addresses, ports, and file types. For procedure, see Configure Logstash Server Information, on page 145.

Step 2 Enable the FileBeat client for remote audit logging. For procedure, see Configure the FileBeat Client, on page 145.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before You Begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Step 4 Repeat this procedure on each node.

Note Do not run any of these commands on all nodes simultaneously.

Platform CLI Commands for Security in EnhancedSecurityMode

When EnhancedSecurityMode is enabled, an administrator can restrict the following options to prevent unauthorized access:

- View audit log
- Download audit log
- Delete audit log
- Enable or disable audit demon

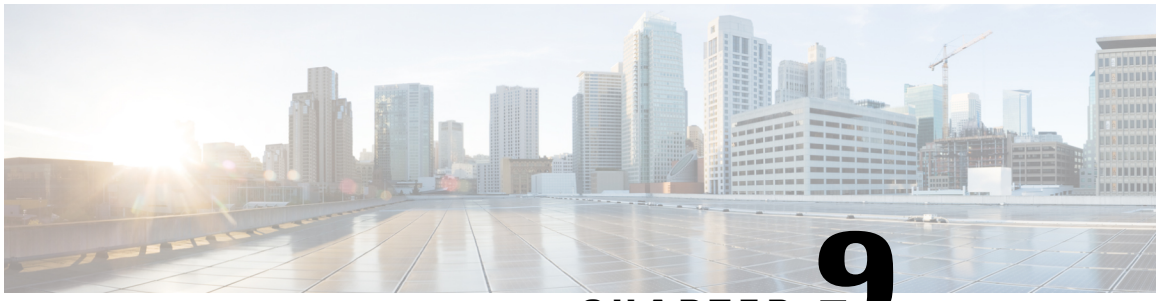
The administrator can restrict the above options by running the following platform CLI commands:

- **file view activelog**<audit log file name>
- **file get activelog** <audit log file name>
- **file delete activelog**<audit log file name>
- **file dump activelog**<audit log file name>
- **file tail activelog** <audit log file name>
- **file search activelog**<audit log file name><search string>
- **file view inactivelog** <audit log file name>
- **file get inactivelog** <audit log file name>
- **file delete inactivelog** <audit log file name>
- **file dump inactivelog** <audit log file name>
- **file tail inactivelog** <audit log file name>
- **file search inactivelog** <audit log file name><search string>
- **utils auditd enable**
- **utils auditd disable**
- **utils auditd status**

Where, <audit log file name> can be one of the following audit log files:

- `/var/log/active/audit/AuditApp`
- `/var/log/active/audit/vos`
- `/var/log/inactive/audit/AuditApp`
- `/var/log/inactive/audit/vos`

Note In a non-EnhancedSecurityMode, the group ownership is ccmsyslog when the permission is 640. However, as part of EnhancedSecurityMode requirement, the file permission is modified to 600 with file group ownership by root. Hence, by default, the files saved at the `/var/log/active/syslog` location are changed to the permission of 600 with the ownership to root.



CHAPTER 9

CTL Update

- More Information, page 149
- Bulk Certificate Management, page 149

More Information

For information about performing a CTL update, see the "Security Basics" section in the *Cisco Unified Communications Manager Security Guide*: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Bulk Certificate Management

Bulk certificate management must be performed manually on both source nodes and destination nodes. The source nodes and destination nodes must be up and running at this point. Phones are registered with the source nodes.

Procedure

Step 1 On the Destination Cluster Publisher, navigate to Cisco Unified Operating System Administration and choose **Security** > **Bulk Certificate Management**.

Step 2 Define the Central Secure File Transfer Protocol (SFTP) server IP address, port, user, password, and directory.

Step 3 Use the **Export** button to export all Trivial File Transfer Protocol (TFTP) certificates from the destination cluster to the central SFTP server.

Step 4 On the Source Cluster Publisher, navigate to Cisco Unified Operating System Administration. Select **Security** > **Bulk Certificate Management**.

Step 5 Define the Central SFTP server with same parameters that you used in Step 2.

Step 6 Click **Export** to export all TFTP certificates from source cluster to the central SFTP server.

Step 7 Click **Consolidate** to consolidate all the TFTP certificates on the central SFTP server. You can perform this step on either the source or destination cluster, using the Bulk Certificate Management interface.

Step 8 On the Source cluster, click **Bulk Certificate Import** to import the TFTP certificates from the central SFTP server.

Step 9 On the Destination cluster, click **Bulk Certificate Import** to import the TFTP certificates from the central SFTP server.

Step 10 Use Dynamic Host Configuration Protocol (DHCP) option **150** to point the phones to the new destination cluster TFTP server.
Upon reset or power cycle, the phones will download the new destination cluster ITL file and attempt to authenticate the new Initial Trust List (ITL) file signature with the certificates in the existing ITL file.

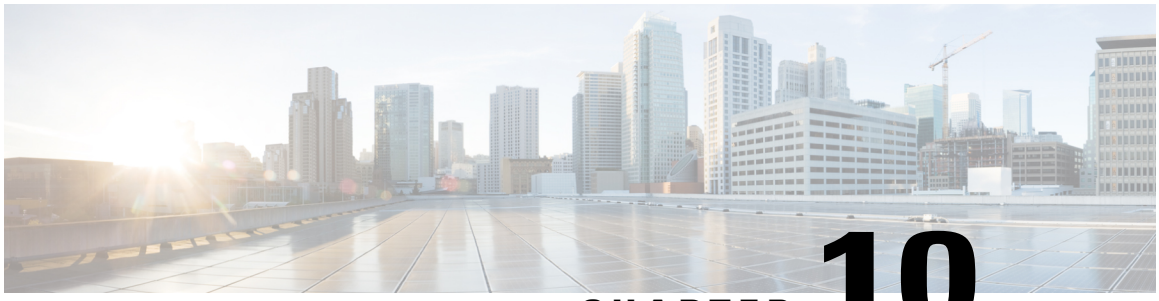
No certificate in the existing ITL file can be used to authenticate the signature, so the phone requests the signer's certificate from the old Trust Verification Service (TVS) server on the source cluster.

The phone sends this request to the source cluster TVS service on TCP port 2445.

The bulk certificate exchange in Steps 1 through 9 provides the TVS service in the source cluster with the TFTP certificate on the destination cluster that signed the new ITL file.

TVS returns the certificate to the phone, which allows the phone to authenticate the signature and replace the old ITL file with the newly downloaded ITL file.

The phone can now download and authenticate the signed configuration files from the new destination cluster.



CHAPTER 10

Best Practices

- Cluster Discovery, page 151
- Upgrades, page 152
- ESXi Host, page 152
- Migration and Installation Virtual Machines, page 152
- Premigration, page 152
- Postmigration, page 153
- Task Validation, page 154
- Cisco Prime Collaboration Deployment Shutdown, page 154
- Monitoring Tasks, page 154
- Managing Files in the SFTP Datastore, page 154
- Using Cisco Prime Collaboration Deployment with Clustering Over WAN , page 155
- Sequence During Migration, page 155
- Server Readdress, page 155
- Fresh Install Publishers and Subscribers, page 155
- Fresh Install of a Unified CM and IM and Presence Cluster , page 155
- Email Notification, page 156
- Test Email, page 156

Cluster Discovery

During cluster discovery, a small Cisco Options Package (COP) file is installed on the servers that are being discovered. For this reason, ensure that before you initiate a discovery, no upgrades or COP file installations are in progress on the servers in the cluster that you want to discover.

Upgrades

When you initiate an upgrade of an application server (Cisco Unified Communications Manager, IM and Presence Service, Cisco Unified Contact Center Express, or Cisco Unity Connection) from the Cisco Prime Collaboration Deployment Upgrade task, the upgrade works in the same manner as upgrades that are initiated by the Unified Communications application GUI or CLI. As a result, we recommend that you follow the same preupgrade procedures and postupgrade verifications as you would directly from the application server GUI.

ESXi Host

Ensure that the virtual machines that you use for migrations or fresh installations reside on an ESXi host that was entered into the Cisco Prime Collaboration Deployment system. That ESXi host should not allow Disaster Recovery System (DRS) or vSphere vMotion.

Migration and Installation Virtual Machines

Always create virtual machines (VMs) for new clusters using the appropriate Open Virtualization Format (OVA) for the unified communications application that you will install. Do not use an existing VM as a destination VM for migration (use a newly-created VM). After a failed migration, if Cisco Prime Collaboration Deployment had started to install the new VM, you must delete this VM and create a new one using the proper OVA.

Note If you have to configure a VMware in various ESXi host servers, ensure that you enter a unique name for ESXi host servers and avoid using the default name from OVA.

Premigration

Source Cluster

- We recommend that you run a full backup by using Disaster Recovery System (DRS) on the cluster.
- We recommend that you check the size of the TFTP folder on the TFTP server. If a number of firmware endpoint COP files was installed on the TFTP server, and if the size of the TFTP directory on the TFTP server is larger than 2.5 GB, we strongly recommend that you delete any large unused firmware files in the `/usr/local/cm/tftp` directory.

The following procedures describe how to check TFTP space usage, and if necessary, how to remove TFTP files on the TFTP server (source node) before you perform a migration using Cisco Prime Collaboration Deployment.

Check TFTP Directory Disk Usage

Procedure

Step 1 Log in using the CLI.

Step 2 Enter the following command: **admin:show diskusage tftp**

Step 3 Check the disk usage output for the following line: **/usr/local/cm/tftp/**. (Disk-usage information appears at the end of the output.)

Step 4 Check the size of the **/usr/local/cm/tftp directory**.

Note We recommend recommended that the size not exceed 2.5 GB. If it does, reduce the size by deleting some files (see procedure below). Before you delete those files, copy them to another server as a backup in case you need them in the future.

Delete TFTP Files

Procedure

Step 1 Log in to the Cisco Unified Operating System Administration GUI on the TFTP server.

Step 2 Navigate to **Software Upgrades** and select **TFTP File Management**.

Step 3 Click **Find** to see a list of TFTP files.

Step 4 Check the check box of the TFTP file that you want to delete.
To delete multiple files, check multiple check boxes.

Step 5 Click **Delete Selected**.

Step 6 After you delete the files, check the disk usage again using the above procedure.

What to Do Next

Note If the cluster has more than one TFTP server, perform these procedures on every TFTP server.

Postmigration

Follow these postmigration best practices:

- Check endpoints

- Check database replication, for example:

```
admin:show perf query class "Number of Replicates Created and State of
    Replication" ==>query class :

- Perf class (Number of Replicates Created and State of Replication)
    has instances and values:

ReplicateCount -> Number of Replicates Created = 676

ReplicateCount -> Replicate_State = 2
```

The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—Replicates were created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Task Validation

If a task is scheduled to start manually or start at a later time, the Validate button appears and you can run validation on the task manually. We recommend that you run the validation on a task before the start (you can run the validation anytime before the start), to identify problems such as missing virtual machines, communication issues, or missing ISO files. When the validation is run, a popup window opens with a list of validation problems. If no problems are found, the following message appears: “All validation tests passed.”

Cisco Prime Collaboration Deployment Shutdown

For best results, to shut down the Cisco Prime Collaboration Deployment server, use the command **utils server shutdown**. Failure to do so can result in Network File System (NFS) mount issues on the ESXi hosts.

Monitoring Tasks

Use the Monitoring GUI page to view the status of your tasks. Click the task in the left column, and the task details appear on the right. Each step in the task (export, install, and so on) appears in the Task Status table below the details section. Click the arrow next to any step to see additional details for that step. Some steps may have several task actions within them. Scroll down to see all the actions and their status.

Managing Files in the SFTP Datastore

The SFTP datastore page shows the ISO and COP files that were transferred to the Cisco Prime Collaboration Deployment server through SFTP. To place a file on the Cisco Prime Collaboration Deployment server, for

use in a migration, install or upgrade task, use an SFTP client and log in as adminsftp (use the administrator password as your password).

When you connect to the Cisco Prime Collaboration Deployment server, upload ISO files to be used by a migration or install task into the `/fresh_install` folder. Upload COP files to the `/upgrade folder`.

After a task is complete, if the ISO is not needed for another task, we recommend that you delete the ISO file from the SFTP datastore to conserve space on your Cisco Prime Collaboration Deployment server. If there are too many ISO files in the SFTP datastore when the Cisco Prime Collaboration Deployment is upgraded or a DRS backup is restored, the Cisco Prime Collaboration Deployment server may run out of space.

Using Cisco Prime Collaboration Deployment with Clustering Over WAN

A minimum bandwidth of 100 Mbps is recommended if the Cisco Prime Collaboration Deployment server and other Unified Communications application nodes are communicating over a WAN.

Sequence During Migration

When you create a migration task, the default sequence is presented, which has one server in each install step. You can use the editing tools in the sequence screen to place more than one server in a step. For best results, include no more than six servers in any one step.

Server Readdress

With the Server Readdress feature, the system inserts a forced pause after each server readdress. Verify that the server was successfully changed and that the phones reregistered before you continue to the next readdress step.

Fresh Install Publishers and Subscribers

When a fresh install task (new UC cluster) includes more than one server, the Cisco Prime Collaboration Deployment system automatically installs the Unified Communications Manager publisher first, and then inserts a forced pause following the publisher installation. During the pause, you can go to the Unified Communications Manager GUI of the newly installed publisher and add the other cluster servers into the **System** > **Servers** GUI. After all the subscribers to be installed in this cluster (Unified Communications Manager subscribers, IM and Presence publishers and subscribers) are added to the Unified Communications Manager publisher GUI, the user can click the **Resume** button on the Cisco Prime Collaboration Deployment Monitoring page to resume the fresh install task.

Fresh Install of a Unified CM and IM and Presence Cluster

When you create a fresh install with both Unified Communications Manager and IM and Presence Service nodes, you must indicate which IM and Presence Service server is the publisher. After the Unified Communications Manager publisher install, the task pauses. This pause allows the subscriber install nodes to

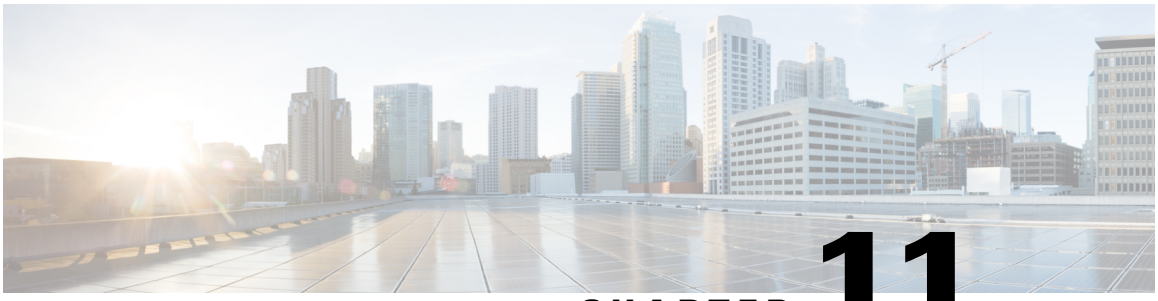
enter into the Unified Communications Manager Publisher (**System** > **Server** GUI page). The IM and Presence Service publisher must be the first IM and Presence server that is added to this list. This step ensures that the IM and Presence Service publisher is installed as the first node.

Email Notification

If a task encounters an error, the task is paused to wait for user intervention. Also, some tasks pause automatically in the task sequence to allow for manual interaction. We recommend that you set up email notification (Standard option) before you run any tasks in order to be notified of pauses or errors that may require your attention when the task runs.

Test Email

When setting up email notification, click the **Send Test email** button to verify that the Cisco Prime Collaboration Deployment mail system can send email to your mail server. Check that the test email was received. Perform this test before you run tasks.



CHAPTER 11

Cisco Prime Collaboration Deployment Troubleshooting

- Increase Disk Space for Migrations, page 157
- General Troubleshooting Issues, page 158
- Errors Seen in View Log, page 158
- Lock Errors, page 162
- NFS Datastores, page 162
- Pause States on Monitor Page, page 162
- Scheduling, page 163
- Server Connectivity, page 163
- Task Failure Due to Restart, page 163
- Task Scheduling, page 172
- Task Timeouts, page 173
- Upgrade Migration and Installation, page 173
- Run a New Task When Current Task in Canceling State, page 174
- Version Validity, page 175
- ISO File Does Not Get Loaded Or Not Recognized During Migration, page 176

Increase Disk Space for Migrations

If one Cisco Prime Collaboration Deployment server is used to migrate a large number of Unified Communications Manager servers concurrently, the Cisco Prime Collaboration Deployment disk can run low on space, and this can cause migration tasks to fail. If you plan to use a Cisco Prime Collaboration Deployment system to migrate several servers concurrently, you can use this procedure to increase the disk size.

Procedure

Step 1 Shut down the Cisco Prime Collaboration Deployment server by logging in to the Cisco Prime Collaboration Deployment CLI and entering the **utils system shutdown** command.

Step 2 After the Cisco Prime Collaboration Deployment server shuts down, go to **ESXi host** and increase the disk size for the virtual machine on which the Cisco Prime Collaboration Deployment server resides.

Step 3 Restart the Cisco Prime Collaboration Deployment server.

Step 4 To view how much disk space is available on the Cisco Prime Collaboration Deployment server, run the CLI command **show status** on the Cisco Prime Collaboration Deployment server.

General Troubleshooting Issues

View Step-By-Step Log of Events

Use the **View Log** buttons on the Monitoring dashboard to see a step-by-step log of Cisco Prime Collaboration Deployment events.

Access Cisco Prime Collaboration Deployment Logs

Obtain additional details by accessing Cisco Prime Collaboration Deployment logs using CLI commands. For example:

file get activelog tomcat/logs/ucmap/log4j/*

Check For Problems Before You Start a Task

Use the **Validate** button to check for problems before starting a task. When the validation process identifies problems, click the **View Log** button to see more detail.

Node Information Mismatches

Some mismatches between node information that is stored in Cisco Prime Collaboration Deployment and the actual node can be fixed automatically (for example, active versions). Other information will require a rediscovery to correct the problem.

Verify Communication Between Servers

Use the **network capture** CLI command to verify communication between servers (for example, to confirm that packets are being sent to and received by the correct ports).

Errors Seen in View Log

The View Log button on the Monitoring dashboard can be used to see a step by step log of Cisco Prime Collaboration Deployment events during the task. When viewing the log, there may be events or errors that are shown. Some of the more common errors, and possible actions to correct those errors, are shown below:

Node Connection and Contact Issues

Error messages:

- "The network diagnostic service indicates node {0} has a network issue. The network settings cannot be changed until the network issue is resolved."
- "The node could not be located."
- "The node could not be contacted. "

Possible actions to correct node connection and contact issues:

- Check the network settings and firewall settings for the indicated node and ensure that the Cisco Prime Collaboration Deployment server can communicate with the node.
- Check to see if the node is powered off, if the node name is misspelled, or if the node is inaccessible.

Other Connection Issues

Error message:

- "The switch version status could not be determined. Please manually verify that the switch version completed."

Possible actions to correct issues:

During a switch version task, if the server does not respond in a fixed amount of time, this message may appear even if the task is successful. you see this error, log in to the CLI for the server that is not responding and run the **show version active** command to see if the switch version was successful. For example, a switch version on a Cisco Unified Contact Center Express server can take more than 60 minutes.

Node Response

Error messages:

- "The node did not respond within the expected time frame."
- "The upgrade service for node {0} did not send back the expected response. This is assumed to be a failure. However, this can also happen when network connectivity is temporarily lost. Please manually verify the upgrade status on node {0} before proceeding."

Possible actions to correct issues:

These messages are usually seen during a task (install, upgrade, and so on), when the new node does not contact the Cisco Prime Collaboration Deployment server within a specified amount of time. For an upgrade, this time is 8 hours, so when one of these error messages appear, it may indicate that the task failed. However, these error messages can also indicate that there were network issues during the upgrade (or install) that prevented the server from contacting Cisco Prime Collaboration Deployment. For this reason, you see one of these messages, log in to the server that is not responding (using the CLI) and run the **show version active** command to see if the upgrade was successful.

Unable to Mount Datastore

Error message:

- "Unable to mount datastore xxx_NFS on ESXi host <hostname>. "

Possible actions to correct the issue:

This error occurs when your Network File System (NFS) Datastore has an issue. Datastore issues can occur when Cisco Prime Collaboration Deployment is shut down unexpectedly. When this error occurs, check the ESXi host and unmount the old NFS mount. Then delete and add back the ESXi host to Cisco Prime Collaboration Deployment.

Unable to Add ESXi Host to Inventory

Possible cause:

This error may be caused by a networking issue with the vSwitch on the ESXi host.

Possible actions to correct the issue:

- Ping the host and verify connectivity by entering the following CLI command: **utils network ping hostname**.
- Verify that the license for the ESXi host is valid. A demo license is not supported.
- Be aware that you need root access to the ESXi host. Use the root username and password when adding ESXi host credentials.
- Be aware that if you are using network address translation (NAT), Cisco Prime Collaboration Deployment and all nodes in the clusters must be behind the same NAT to ensure successful communication between Cisco Prime Collaboration and the nodes.

Unable to Power On Virtual Machine

Error message:

- "Unable to power on the VM named xxx on ESXi host xxxxxxx. "

Possible actions to correct issue:

Check the ESXi host that the VM resides on. From the **Tasks and Events** tab, check the time stamp for when Cisco Prime Collaboration Deployment tried to power on the VM. Determine whether too many VMs are already on that host. If that is the case, you may need to power off a VM that is not being used for this cluster.

The Power State of a Virtual Machine

Error message:

- "The power state of VM xxxxx in ESXi host XX.XX.X.XX needs to be OFF. The task is now paused."

Possible actions to correct issue:

VMs that are to be used in a destination cluster for a migration task, or for a new cluster installation, must be in the OFF state. If you receive this error message, check the named VM. If it is not off, power it off. Then, retry or resume the task.

Username and/or Password Not Valid

Error message:

- " The username and/or password is not valid."

Possible actions to correct the issue:

Correct the administrator name and password for this server in the cluster page. You can then rediscover this node.

Platform Administrative Web Services (PAWS)

Error messages:

- "The Platform Administrative Web Services (PAWS) is not available."
- " Unable to access node {0} via the Platform Administrative Web Services (PAWS) interface."

Possible actions to correct issues:

Ensure that the server is reachable, and that the PAWS service is active on the node. When you use Cisco Prime Collaboration Deployment to perform an upgrade, switch version, or restart task on an application server (for example, to upgrade a Unified Communications Manager server), the Platform Administrative Web Service on the application must be active. Otherwise, the Cisco Prime Collaboration Deployment server cannot communicate with the Unified Communications Manager application server.

{0} VMs Named {1} Were Located on ESXi Host {2}

Error message:

- " {0} VMs named {1} were located on ESXi host {2}."

Possible actions to correct issue:

Check that the virtual machine named still exists on the ESXi host. Sometimes VMs are moved to another ESXi host, and if this is the case, the ESXi host that holds the VM must be added into the Cisco Prime Collaboration Deployment server.

Power State of VM {0} in ESXi Host {1} Needs to Be OFF

Error message:

- "The power state of VM {0} in ESXi host {1} needs to be OFF."

Possible actions to correct the issue:

In order for Cisco Prime Collaboration Deployment to be installed on or migrate to a VM, the power state of the target VMs must be OFF.

CLI Command Timed Out

Error message:

- "CLI command timed out for node {0}."

Possible actions to correct issue:

Check for networking, connection, or password issues with the node. Also check to see if another operation was in progress (for example, a COP file install) during the time that the command timed out.

Task Paused Due to Validation Issues

Error message:

- " Task paused due to validation issues"

Possible actions to correct the issue:

Before it runs a task, the Cisco Prime Collaboration Deployment server will run validation checks to ensure that VMs to be used are available, that the ISO file can be found, and so on. This message indicates that one or more of the validation checks failed. See the log file for more information about which validations failed.

Lock Errors

Most products allow only one change at a time (for example, you cannot modify Network Time Protocol settings while an upgrade is in progress). If a request is made while the node is locked, then a lock message with the following information is displayed:

- The name of the resource that was locked
- The ID of the process that locked the resource
- The hostname of the node

You can typically wait a few minutes and try again. For more details, use the node CLI to identify the exact process based on the provided process ID and hostname.

NFS Datastores

Exceptions and Other NFS-Related Issues

Review the Cisco Prime Collaboration Deployment logs for any exceptions or other NFS-related issues.

Use VMware vSphere

Use VMware vSphere to verify that NFS datastores are available.

Unmount and Remount All Current Datastores

When you restart it, Cisco Tomcat unmounts all current datastores and attempts to remount them.

Pause States on Monitor Page

Task Is Waiting for Manual Intervention

Certain tasks, such as migration or readdress, pause at a point that human intervention may be required. In those tasks, the Cisco Prime Collaboration Deployment system inserts a Forced Pause. When the task reaches this point, the task is paused and a message appears on the Monitoring page. Perform manual steps as needed, and then click the **Resume** button when you are ready to resume the task.

Task Paused Due to Validation Issues

When this message is displayed, click the **View log** link to view more detail on which validations failed.

Task Paused Due to Task Action Failures

When this message is displayed, click the **View log** link to view more detail on which tasks failed.

Scheduling

Verify Scheduled Date

If a task was scheduled but did not start, verify the scheduled date.

Validation Tests

When a task starts, Prime Collaboration Deployment runs a series of validation tests. A validation failure pauses the task.

Determine Why a Task Has Been Paused

Use the **View Log** button to see why a task is paused (for example, validation failure, a requested or required pause, one or more nodes failed on a partiular step, and so on).

Canceled Tasks

Some steps cannot be canceled after they are started (for example, restarting a server).If you cancel the task, it remains in the Canceling state until the step is finished.

Server Connectivity

Verify Connectivity

Use the **utils network ping** and **traceroute** CLI commands to verify connectivity.

Verify Forward and Reverse DNS Lookups

Use the **utils network host** CLI command to verify forward and reverse DNS lookups.

Platform Administrative Web Services

Ensure that Platform Administrative Web Services are activated on nodes that are being upgraded, restarted, and switch versioned.

Verify That Ports Are Open

Verify that the ports listed in the **Port Usage** guide are open (for example, verify that the NFS and SOAP call-back ports are not being blocked by other network devices).

Task Failure Due to Restart

The success or failure of each of the following tasks depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the task. If connectivity to the servers is

lost, or if the Prime Collaboration server reboots during a task, the task might show a failure even though it may have completed successfully.

Installation Task Failure

Problem

The success or failure of each step in the install task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the installation.

Possible Cause

If the Prime Collaboration server reboots during the install task, the installation might show a failure, even though it may have completed successfully.

The following table describes the steps to identify if the task completed successfully on the application server, and, if it did not, how to recover from this type of failure.

Solution

Table 14: Example Deployment: Multinode Cluster Deployment

If	Then
The failure occurs during installation on the first node	**1** You must create a new fresh-install task with the same cluster nodes. **Note** In the case of Unified Communications products such as Cisco Unified Communications Manager and IM and Presence Service, Cisco Prime Collaboration Deployment does not support an install task that installs a subsequent node separately from the cluster. **2** Check the status of the VM on the ESXi host that is associated with the destination cluster. If any VMs were powered on and installed, delete those VMs and redeploy the OVA. **Note** For more information, see topics relating to install tasks.

If	Then
The installation is successful on the first node but fails on any of the subsequent nodes after Prime Collaboration Deployment loses connectivity	1 Log in to the failed Unified Communications VM node, such as Cisco Unified Communications Manager, and manually verify the installation status. For more information, see Unified Communications product documentation. 2 Create a new install task with all new cluster nodes. You must restart the installation process by deleting all installed VMs, redeploying the recommended OVA to create new VMs, and creating a new install task. **Note** If VM names are changed from previous configuration, you must add a new fresh install cluster, create a new fresh install task, and then run the task. 3 Check the status of the VM on the ESXi host that is associated with the destination cluster. If any VMs were powered on and installed, delete those VMs and redeploy the OVA. **Note** For more information, see topics relating to install tasks.

Upgrade Task Failure

Problem

The success or failure of each step in the upgrade task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the upgrade.

Possible Cause

If the Prime Collaboration server reboots during an upgrade task, the upgrade might show a failure even though the upgrade may have completed successfully.

The following table describes the steps to determine whether the task completed successfully on the application server and, if it did not, how to recover from this type of failure.

Solution

Table 15: Example Deployment: Multinode Cluster Deployment

If	Then
The failure occurs during upgrade on the first node	**1** Check task status on the **Monitoring** page to see which steps were successful and which steps failed. **2** Log in to the first Unified Communications VM node, such as Cisco Unified Communications Manager. Check the software version and upgrade status to verify whether this node was upgraded to a new version. For more information, see Unified Communications product documentation. **3** If the upgrade on the first node is successful, you can create a new upgrade task with the subsequent node. **4** If the upgrade on the first node is unsuccessful, you can create a new upgrade task with all nodes. **5** If the upgrade task was configured with automatic switch version, check the status of the active and inactive partitions on the Unified Communications product node. If the automatic switch version was unsuccessful on the Unified Communications product node, perform a switch version. For more information, see Unified Communications product documentation. **Note** If the switch version is required, this must be done before you a new upgrade task with subsequent nodes with a new upgrade task that is configure with auto-switch version. **Note** If you create an upgrade task to install a COP file, verify COP-file installation status directly on the Unified Communications node.

If	Then
The upgrade is successful on the first node but fails on any of the subsequent nodes after Prime Collaboration Deployment loses connectivity	1 Log in to the failed Unified Communications VM node, such as Cisco Unified Communications Manager. Check the software version and upgrade status to verify whether this node was upgraded to a new version. For more information, see Unified Communications product documentation. **Note** If the subsequent node shows the correct new version, you do not need to recreate an upgrade task on Prime Collaboration Deployment. 2 If the subsequent node shows the new version in the inactive partition, the old version in active partition, and the upgrade task was configured to switch version automatically, you must either perform the automatic switch version manually on the Cisco Unified Communications Manager node or use Prime Collaboration Deployment to create a switch version task. 3 If the upgrade task was configured with automatic switch version and the subsequent node does not show the version correctly, perform a switch version. See Unified Communications product documentation more detail. **Note** If you created an upgrade task to install a COP file, verify COP-file installation status directly on the Unified Communications node.

Migration Task Failure

Problem

The success or failure of each step in the migration task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the migration.

Possible Cause

If the Prime Collaboration server reboots during the migration task, the migration might show a failure even though it may have completed successfully.

Solution

If the migration task fails after Prime Collaboration Deployment loses connectivity, we recommend that you restart the entire migration process. To restart the migration task, you must create a new task. If your deployment is a multinode cluster, follow this procedure:

1. Check the task status on the **Monitoring** page to find out which steps were successful and which steps failed.
2. If the source node was shut down, you must power on the node manually.

Note Repeat this step for all source nodes that were shut down.

3. Delete the failed migration task.
4. Delete the destination migration cluster that is associated with the failed migration task.

Note You do not need to delete the source cluster.

5. Check the status of the VM on the ESXi host that is associated with the destination cluster. If any VMs were powered on and installed, delete those VMs and redeploy the OVA.

Note For more information, see topics relating to migration tasks.

Switch Version Task Failure

Problem

The success or failure of each step in the switch version task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the switch version.

Possible Cause

If the Prime Collaboration server reboots during the switch version task, the switch version might show a failure even though the switch version may have completed successfully.

The following table describes the steps to determine whether the task completed successfully on the application server, and, if it did not, how to recover from this type of failure.

Solution

Table 16: Example Deployment: Multinode Cluster Deployment

If	Then
The failure occurs during switch version on the first node	1 Log in to the first Unified Communications VM node (for example, Cisco Unified Communications Manager) and manually check the sofware version in both the active and inactive partitions. For more information, see Unified Communications product documentation. 2 If the first node still shows the old version in the active partition but the new version in the inactive partition, create a new switch version task with the same nodes on Prime Collaboration and run the task again.
The switch version is successful on the first node but fails on any of the subsequent nodes after Prime Collaboration Deployment loses connectivity	1 Log in to the subsequent Unified Communications VM node (for example, Cisco Unified Communications Manager). Check the software and switch version status to verify that the subsequent node is up and running with the correct version. 2 If the subsequent node shows the correct new version in the active partition, you do not need to recreate a switch version task on Prime Collaboration Deployment. 3 If the subsequent node shows the new version in the inactive partition and the old version in active partition, the switch version was not successful on the subsequent node. You can either perform a switch version manually on the subsequent node or create a new switch version task on the subsequent node on Prime Collaboration Deployment.

Readdress Task Failure

Problem

The success or failure of each step in the readdress task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster.

Possible Cause

If the Prime Collaboration server reboots during the readdress task, you may be notified of a failure even though the readdress may have completed successfully.

The following table describes the steps to determine whether the task completed successfully on the application server, and, if it did not, how to recover from this type of failure.

Solution

Table 17: Example Deployment: Multinode Cluster Deployment

If	Then
The failure occurs during readdress on the first node	**1** Log in to the first Unified Communications VM node (for example, Cisco Unified Communications Manager) and verify that network settings were successfully changed. For more information, see Unified Communications product documentation. **2** After you verify that network settings were successfully changed on the first node, create a new readdress task on the subsequent node on Prime Collaboration Deployment and run this task. If network settings were not successfully changed on the first node, create a new readdress task with both nodes on Prime Collaboration Deployment and run the task again.

If	Then
The readdress task is successful on the first node but fails on any of the subsequent nodes after Prime Collaboration Deployment loses connectivity	1 Log in to the first Unified Communications VM node (for example, Cisco Unified Communications Manager) and verify that network settings were successfully changed. For more information, see Unified Communications product documentation.. 2 After verifying that network settings were successfully changed on the first node, you do not need to create a new readdress task on the first node on Prime Collaboration Deployment. However, you do need to create a new readdress task on the subsequent nodes. If network settings were not successfully changed on the first node, create a new readdress task with the first node and subsequent nodes on Prime Collaboration Deployment and run the new task. 3 If network settings were successfully changed, update cluster discovery for this cluster to make sure that Prime Collaboration Deployment has the correct network settings. 1 Go to the **Clusters** screen and click the triangle to show the nodes in the cluster. 2 Check the network settings to ensure that the Cluster Nodes table shows the new network settings (for example, hostname). 3 If the correct network settings are not displayed, click the **Refresh Node** link for each node in the cluster.

Server Restart Task Failure

Problem

The success or failure of each step in the server restart task depends on the Prime Collaboration Deployment server being able to get a response from every server in the cluster during the server restart.

Possible Cause

If the Prime Collaboration server reboots during server restart, the server restart might show a failure, even though the server restart may have completed successfully.

The following table describes the steps to determine whether the task completed successfully on the application server, and, if it did not, how to recover from this type of failure.

Solution

Table 18: Example deployment: Multi-node cluster deployment

If	Then
The failure occurs during server restart on the first node	1 Log in to the first Unified Communications VM node (for example, Cisco Unified Communications Manager) and manually check the status of the restart. 2 If the first node did not get restarted, recreate a new server restart task with all nodes and run the task again.
The server restart is successful on the first node but fails on any of the subsequent nodes after Prime Collaboration Deployment loses connectivity	1 Log in to the second Unified Communications VM node (for example, Cisco Unified Communications Manager) and manually check the status of restart. 2 If the subsequent node restarted successfully, there is no need to recreate a new server restart task. If the subsequent node did not restart, create a new server restart task on the subsequent node only.

Task Scheduling

Task Scheduled but Not Started

If a task was scheduled but did not start, verify the scheduled date.

Validation Failure

When a task starts, a series of validation tests are run. A validation failure pauses the task.

Reasons for a Task Pause

Click the **View Log** button to see why a task was paused (for example, validation failure, a pause was requested or required,, one or more nodes failed on a particular step, and so on).

Tasks That Cannot Be Canceled

Some tasks cannot be canceled once started (for example, restart of a server or installation of a server node). If the task is canceled, it remains in the Canceling state until the step is finished.

Task Timeouts

Manually Verify Results

All Cisco Prime Collaboration Deployment tasks have built-in timeouts ranging from 30 minutes to 10 hours, depending on the type of task and product. If Cisco Prime Collaboration Deployment does not receive the expected results within that time frame, Cisco Prime Collaboration Deployment signals an error, even if the actual process succeeded. Users must manually verify the results and ignore any false negatives.

Readdress Times Out

During readdress, if a VLAN change is required, Cisco Prime Collaboration Deployment does not receive updates for the nodes. As a result, the readdress eventually times out even though the actual readdress process succeeded.

Resource Issues Slowing Down the Nodes

Use VMware vSphere to verify that no resource issues are slowing down the nodes. Disk, CPU, and memory issues can cause slower than normal logins, which can cause connectivity timeout issues during cluster discovery.

Network Congestion

Because large files are sent across the network during upgrades, installations, and migrations, network congestion can cause tasks to take longer than usual.

Upgrade Migration and Installation

Virtual Machine Does Not Boot

If a VM does not boot using the mounted install ISO during migration or installation, verify the VM boot order in the Basic Input/Output System (BIOS). We recommend that only freshly created VMs that use the official Cisco Open Virtualization Format (OVF) files.

VM Cannot Be Located

If a VM cannot be located, make sure vMotion is turned off.

Upgrade File List Is Blank

If the list of ISO files for upgrade is blank, the reason might be that one or more servers in the cluster you are upgrading have an existing upgrade that is stuck. The file list shows as blank because the Unified Communications Manager-side upgrade process was stuck. Therefore, no files are valid, because no upgrades can be done. If you attempt an upgrade from the application server CLI, you may see the message “The resource lock platform.api.network.address is currently locked.”

To resolve this problem, reboot your Unified Communications Manager server.

Upgrade ISO or COP File Is Not Displayed in the Task Wizard

If an upgrade ISO or COP file is not displayed in the task wizard, verify that the file was uploaded into the correct directory on the Prime Collaboration Deployment Server. To confirm the location of the file, click open and close navigation button and choose the **Inventory** > **SFTP Servers and Datastore** menu option. The directory that is in use is usually listed at the top of the task wizard.

Upgrade ISO File Must Be Valid for All Nodes

An upgrade ISO file must be valid for all nodes in the task in order to be listed in the wizard. If the upgrade ISO file is not listed, verify that the task contains the publisher or that the publisher was already upgraded.

Release 10.x and Older Products

Most Release 10.x and older products report only generic upgrade and installation failure messages. Users must access the failed node directly and diagnose the problem by using traditional tools and processes that are specific to that product (for example, use the Unified Real-Time Monitoring Tool or the CLI to view upgrade logs).

Run a New Task When Current Task in Canceling State

Rerun Fresh Install Task

The following procedure provides the high-level steps for rerunning a new task when the current task is in the process of being canceled. For more detailed information, see topics relating to task management.

Procedure

Step 1 View the task log to verify the status of the most recent task.

a) If the VM is powered on and the fresh install task is still in progress, power off the VM, delete it, and redeploy the OVA to create a new VM. You can use the same name for the new VM.

b) If the VM is powered off and the fresh install was not started on the VM, leave the VM powered off.

Step 2 Check the cluster to verify if any nodes in the cluster were updated with the active version and discovery status.

- If any nodes were updated with the new version or discovery status, create a new cluster with a new name, including the same VMs and installation settings.
- If any nodes in the cluster were not updated, reuse the cluster when recreating a fresh install task.

Step 3 Create and run a new install task.

Rerun Migration Task

The following procedure provides the high-level steps for rerunning a migration task for the same source and destination clusters when the current migration task is in the process of being canceled. For more detailed information, see topics relating to task management.

Procedure

Step 1 View the task log to verify the status of the most recent task.

a) If the VM is powered on and the migration task is still in progress on the destination VM, power off the destination VM, delete it, and redeploy the OVA to create a new destination VM. You can use the same name for the new VM.

b) If the VM is powered off and the migration was not started on the VM, leave the VM powered off.

Step 2 Check the node status on the source cluster before running a new task.

- If the source node is powered off, power on the source node and make sure it is in a running state before rerunning a migration task.
- In the case of network migration, the source node can remain powered on.

Step 3 You do not need to rerun cluster discovery on the source node.

Step 4 Check the destination cluster to ensure that no nodes were updated with active version or discovery status.

- If any nodes in the destination cluster were updated with the new version of application or discovery status, create a new migration destination cluster by giving it a new name with the same source cluster and select the same destination VMIf any nodes in the destination cluster have been updated with the new version of application or discovery status, create a new migration destination cluster by giving it a new name with the same source cluster and select the same destination VMs.
- If any nodes in the destination cluster were not updated with the new version of application or discovery status,you may be able to reuse the migration destination cluster later when creating a new migration task. If this is not possible, recreate a migration destination cluster with a new name.

Step 5 Create a new migration task with the same source cluster and new destination cluster.

Step 6 Start running the new task.

Version Validity

Install or migrate Cisco Prime Collaboration Deployment if the version validity is True for the Restricted or Unrestricted version of Cisco Prime Collaboration Deployment.

Table 19: Supported Tasks based on Version Validity

From	To	Version Validity
Export Restricted (K9)	Export Restricted (K9)	True

From	To	Version Validity
Export Restricted (K9)	Export Unrestricted (XU)	False
Export Unrestricted (XU)	Export Restricted (K9)	True
Export Unrestricted (XU)	Export Unrestricted (XU)	False

ISO File Does Not Get Loaded Or Not Recognized During Migration

When you create a migration task to upgrade and migrate a cluster to new virtual machines, the task extracts the information from the old servers and starts the virtual machines. In case, the ISO file either does not get loaded or is not recognized, perform the following steps:

1. On Cisco Unified Communications Manager virtual machine, verify the correct ESXi BIOS boot order of the Cisco Unified Communications Manager virtual machine. For example, CDROM, removeable devices, hard disk drive (HDD), and network boot from VMXNET3.
2. Verify the ESXi host of Cisco Unified Communications Manager virtual machine by using ESXi Foundation or Standard or higher.

Note Hypervisor edition does not enable ESXi APIs that Cisco Prime Collaboration Deployment requires.

3. Verify that Cisco Prime Collaboration Deployment has root access to ESXi host.
4. Verify that the NFS mount is stable.
   - If ISO file does not mount to virtual machine from NFS, check **ESXihost** > **config** > **storage (datastore)** > **storage (datastore)**.

     Note If the datastore is inactive, you need to reconnect it.

   - To force reconnection of NFS mount, through Cisco Prime Collaboration Deployment, remove the ESXi host and add it again. Then, rerun the migrate task.