Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 14

First Published: 2020-11-19

Last Modified: 2025-12-02

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

© 2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Installing Cisco Unity Connection** 1

- Introduction 1
- Methods of Installation 1
- Important Considerations for Installation 2
- Install with Data Import 3
- Pre-Installation Tasks 4
  - Creating a Virtual Machine 5
  - Changing the Boot Order of Virtual Machine 6
  - Changing Reservation on Virtual Machines Running with E7 or E5 Processors 6
    - Changing the Reservation Numbers 7
  - Verifying DNS Settings 7
  - Gathering Information for Installation 7
- Installation Scenarios 12
- Installation Tasks 13
  - Navigating Within the Installation Wizard 13
  - Installing the Publisher Server 13
  - Configuring Subscriber Server on the Publisher Server 17
  - Installing the Subscriber Server 17
  - Generating Answer File for Unattended Installation 18
    - Task List for Unattended Installation 19
  - Touchless Installation for Virtual Machine 20
    - Methods for Touchless Installation 20
    - Task List for Touchless Installation 21
    - (Optional) Enabling Dynamic-Cluster-Configuration Using CLI 22
  - Automated Installation using vApp properties and VMware OVF Tool 22
    - Task List for Manual Installation using vApp Options 23

Task List for Touchless Installation using VM Tools 23
Applying a Patch 24
Upgrading from a Remote Server 25
Upgrading from a Local Disk 27
Verifying the Installation 27
Cisco Unity Connection Survivable Remote Site Voicemail Installation 28
Post-Installation Tasks 29
Post-Migration Tasks 29
Troubleshooting Installation Issues 32

CHAPTER 2 **Backing Up and Restoring Cisco Unity Connection Components** 33
About Cobras 33
About Disaster Recovery System 33
Components Supported for DRS Backup 34
Backup Files in DRS 34
Configuring DRS Backup 35
Configuring a Backup Schedule 36
Configuring a Manual Backup 37
Viewing the Backup Status 37
Viewing the Backup History 38
Configuring DRS Restore 38
Viewing the Restore Status 40
Viewing the Restore History 40
About System Restore Tool 40
Types of System Restore Points 41
Creating a Restore Point task 41
Enabling Create Backup Restore Point 41
Restoring Data using Restore Points task 42

CHAPTER 3 **Upgrading Cisco Unity Connection** 43
Introduction 43
Upgrade Types 43
Status of Unity Connection Cluster During an Upgrade and Switch version 47
Duration of Upgrade 48

Prerequisites for Upgrade 48
Upgrade Considerations with FIPS Mode 51
Task list to Upgrade to Unity Connection Shipping Version 14 51
Upgrading the Unity Connection Server 55
Switching to the Upgraded Version of Unity Connection Software 57
Applying COP file from a Network Location 58
Rollback of Unity Connection 59
Rollback Scenarios 59
Rollback a Unity Connection Server to the Version in the Inactive Partition 60

CHAPTER 4 **Configuring Cisco Unity Connection Cluster** 61
Introduction 61
Task List for Configuring a Unity Connection Cluster 61
Administering a Unity Connection Cluster 62
Checking the Cluster Status 62
Steps to Check Unity Connection Cluster Status from Command Line Interface (CLI) 62
Managing Messaging Ports in a Cluster 63
Stopping All Ports from Taking New Calls 64
Restarting All Ports to Take Calls 65
Server Status and its Functions in a Unity Connection Cluster 65
Changing Server Status in a Cluster and its Effects 68
Manually Changing the Server Status from Secondary to Primary 68
Manually Changing from the Server Status from Secondary to Deactivated 68
Manually Activating a Server with Deactivated Status 69
Effect on Calls in Progress When Server Status Changes in a Unity Connection Cluster 69
Effect on Unity Connection Web Applications When the Server Status Changes 70
Effect of Stopping a Critical Service on a Unity Connection Cluster 70
Shutting Down a Server in a Cluster 71
Replacing Servers in a Cluster 72
How a Unity Connection Cluster Works 72
Effects of Split Brain Condition in a Unity Connection Cluster 73

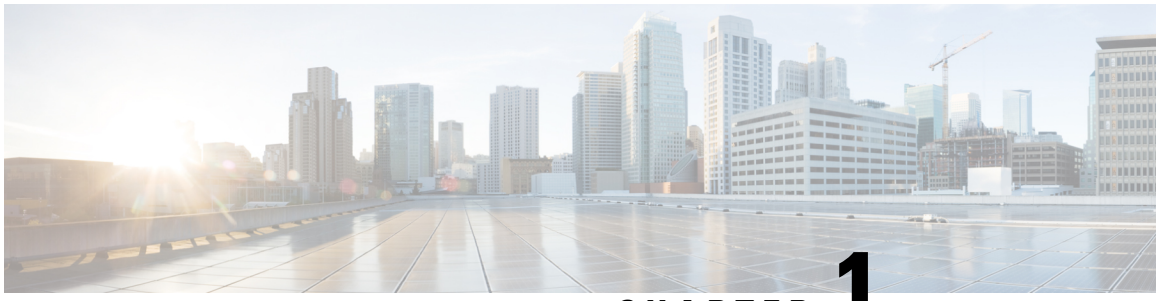
CHAPTER 5 **Maintaining Cisco Unity Connection Server** 75
Migrating a Physical Server to a Virtual Machine 75

Replacing a Publisher Server 76
Replacing a Subscriber Server 77
Replacing the Non-Functional Server 78
Changing the IP Address or Hostname of a Unity Connection Server 79
Determine Whether Unity Connection is Defined by Hostname or IP Address 80
Important Considerations before Changing the Hostname or IP Address of a Unity Connection Server 80
Changing the IP Address or Hostname of a Unity Connection Server or Cluster 81
Adding or Removing Unity Connection Languages 83
Task List for Adding Languages to a Standalone Unity Connection Server 84
Installing Unity Connection Language Files from Network Location or Remote Server 84
Removing Unity Connection Language Files 86

CHAPTER 6 **Managing Licenses** 87
Managing Licenses 87
Overview 87
Deployment Options 88
Smart Account and Virtual Account 88
Prerequisites for Configuring Cisco Smart Software Licensing 89
Configuring Cisco Smart Software Licensing in Unity Connection 89
Configuring Transport Settings (optional) 89
Token Creation 90
Registering the Unity Connection 90
Managing Cisco Smart Software Licensing 91
Smart Software Licensing Status 91
Registration Status 91
Authorization Status 92
License Reservation in Unity Connection 92
Configuring Specific License Reservation in Unity Connection 93
Configuring Permanent License Reservation in Unity Connection 93
License Reservation Status 94
Enforcement Policy on Unity Connection 95
Licenses in Unity Connection Cluster 96
Migrating Licenses 96

Enabling Encryption in Cisco Unity Connection 96
License Parameters for Unity Connection Features 98

CHAPTER 7 **Managing Cisco Unity Connection using Cisco Prime Collaboration** 101
Managing Cisco Unity Connection using Cisco Prime Collaboration 101



CHAPTER 1

Installing Cisco Unity Connection

- Introduction, on page 1
- Methods of Installation, on page 1
- Important Considerations for Installation, on page 2
- Install with Data Import, on page 3
- Pre-Installation Tasks, on page 4
- Installation Scenarios, on page 12
- Installation Tasks, on page 13
- Post-Installation Tasks, on page 29
- Post-Migration Tasks, on page 29
- Troubleshooting Installation Issues, on page 32

Introduction

Cisco Unity Connection can be deployed in either of the following ways:

- Standalone Deployment: Involves the installation of a Unity Connection as a single server.
- Cluster Deployment: Involves the installation of same version of two Unity Connection servers in an active-active or high availability mode. During the installation of Unity Connection as a cluster, the first server is referred to as publisher server and the second server as the subscriber server. For more information on cluster configuration, see the Configuring Cisco Unity Connection Cluster chapter.

Note Unity Connection 10.0(1) and later releases can only be installed on virtual machines. For more information, see the http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html.

Methods of Installation

You can use either of the following methods to install standalone or cluster server:

- **Standard Installation**: Allows you to manually specify the installation information, such as hostname and IP address using installation wizard.

- **Unattended Installation**: Allows you to install Unity Connection using an installation disk and a pre-configured answer file floppy diskette. The answer file has all the information required for unattended installation. Unattended installation is a seamless process of installation that allows you to start installation on both the publisher and subscriber servers simultaneously. The subscriber installation continues when the publisher is successfully installed. This type of unattended installation is Touchless Installation. For more information on Touchless Installation, see the Touchless Installation for Virtual Machine.

Note

- You can also perform fresh installation of Unity Connection 14 and later using Cisco Prime Collaboration Deployment. For more information on Cisco PCD, see http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html
- The answer file supports only fresh installs and does not support upgrades.

- **Install with Data Import**: Cisco Unity Connection 14SU1 and later releases, supports installation of Unity Connection along with the data import from the previous releases. It involves migration of data by exporting source release data to SFTP server, and installing a new machine with import of that data. Examples of data that you can export and import are component specific configurations files, voicemails, DB related files, platform provision data and platform files like certificates. For more details, see Install with Data Import section.
- **Automated Installation using vApp properties and VMware OVF Tool**: Cisco Unity Connection 14SU2 and later releases, supports automated installation of Unity Connection via VMware Open Virtualization Format(OVF) Tool. The VMware OVF Tool is used to deploy and inject the Unity Connection configuration parameters into the virtual machines using skip-install OVA and vApp properties without using Answer File Generator or vFloppy images. For more details, see Automated Installation using vApp properties and VMware OVF Tool section.

Important Considerations for Installation

Before you proceed with the installation, consider the following points:

- Verify the system requirements, such as licensing and phone integration requirements necessary for the Unity Connection server in the System Requirements for Cisco Unity Connection guide at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.
- Be aware that when you install on an existing Unity Connection server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Ensure that you connect each Unity Connection server to an uninterruptible power supply (UPS) to provide power backup and protect your system. Failure to do so may result in damage to physical media and require a new installation.
- Ensure that the virtual machine has ESXi 7.0 U1 and VM version 13 and above.
- For a Unity Connection cluster:
  - Install the Unity Connection software first on the publisher server and then on the subscriber server (applicable to only standard installation scenarios). For more information on installation scenarios, see Installation Scenarios.

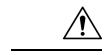
- Note down the Security password that you mention at the time of installing publisher server. You need to specify the same password when installing the subscriber server in a cluster.
- Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between the publisher and subscriber servers.

- Verify that DNS server is properly configured before installing Unity Connection. For more information, see the Verifying DNS Settings.
- Do not perform any configuration changes during the installation.
- Be aware that the directory names and filenames that you enter during the installation are case-sensitive.

Install with Data Import

When the migration cluster is created using **Install with Data Import** installation method, you must indicate whether all destination cluster nodes will keep the same hostname or IP address, or if some of these addresses will be changing. Depending upon this there are two types of Data Migration as explained below:

- **Simple Migration**: Using the source node settings for all destination cluster nodes is referred to Simple Migration.
- **Network Migration**: Entering new network settings for one or more destination cluster nodes is referred to Network Migration.



Caution

1. If Intrasite, HTTPS and SRSV networking is configured remove the server from the Unity Connection site before performing Install with Data Import. For instructions, see the Networking Guide for Cisco Unity Connection Release 14 available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/networking/guide/b_14cucnetx.html.
2. If Google Workspace is configured with Unity Connection, save and reset the Google Workspace unified messaging service on Unity Connection after performing Install with Data Import. Also disable the Google Workspace unified messaging service from Unity Connection where data export CLI was executed before performing data import to prevent message duplicacy. For instructions, see section Task List for Configuring Unified Messaging with Google Workspace of the *Unified Messaging Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/unified_messaging/guide/b_14cucumgx.html

Following are the different ways to perform Install with Data Import:

1. Export data from source publisher node, Import data on destination publisher node and fresh install destination subscriber node.
2. Export data from both source publisher and subscriber nodes and import data on both destination nodes.

Note Data exported from Publisher Node cannot be imported on the Subscriber Node.

You can perform Export and Import of data by the following steps:

1. Run the pre-upgrade-check COP file, and install the COP file **ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512** on both the nodes of cluster , if it is recommended by the pre-upgrade check report otherwise skip this step.
2. *(Applicable for Unity Connection 14 release)* Install the COP file **ciscocm.cuc_DataExport_v1.1.k4.cop.sha512** on both nodes of cluster.
3. You can use below CLI command to export source release data:

   ```
   utils system upgrade dataexport initiate
   ```

   Execute above CLI command on publisher node to export data. Export subscriber node data only after completion of export on publisher node as per requirement. For more information on CLI usage, see "Utils Commands" chapter of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

   Please note the following information related to CLI:

Note

- It is recommended to execute this CLI during Off hours to avoid voicemail impact. While CLI execution is in progress, you will not be able to access voicemails and send messages.
- It is available on Unity Connection 14SU1 and later releases therefore COP installation step is not required.
- It will continue to run in background in case of any network disconnect on Unity Connection 14SU1 and later releases. For Unity Connection Release 14, CLI will terminate in case of network disconnect.

4. Import data on new virtual machines of release 14SU1 or later, using Import option available in Installation wizard. For more information see Installing the Publisher Server, on page 13 section.

Note

1. Make sure to install **ciscocm.cuc_preUpgradeCheck-001.k3.cop.sgn** COP on both nodes of the cluster and verify that the cluster is ready for migration before Data Export. Download the COP files from https://software.cisco.com/download/home/286313379/type/286319537/release/COP-Files.
2. Make sure that the server on which Import is to be performed is created using recommended OVA. For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html.
3. Once migrated, if for any reason you decide to roll back Data Export COP file on Unity Connection 14 Release, then install **ciscocm.cuc_DataExport_rollback_v1.1.k4.cop.sha512** COP file.

Pre-Installation Tasks

Before installing a Unity Connection server, you need to understand all the pre-installation steps as well. The Table 1-1 contains a list of pre-installation tasks that you must consider to ensure successful installation of Unity Connection server.

Table 1: Pre-Installation Tasks

	Task	Important Notes
Step 1	Ensure that your servers are listed as supported hardware and sized appropriately to support the load of the cluster.	For information about the capacity of serv the link http://www.cisco.com/c/dam/en/us/docs/voice_ip_comm/cuc_system/virtualization/virtual
Step 2	Create the virtual machine using the correct OVA template.	For more information, see the Creating a Vi section.
Step 3	Change the boot order of the virtual machine to update the BIOS settings.	For more information, see the Changing th of Virtual Machine section.
Step 4	Configure an external NTP server during a Unity Connection server installation. For a Unity Connection cluster, the NTP server helps to synchronize time between publisher and subscriber server. Ensure the external NTP server is stratum 9 or higher (meaning stratums 1-9). The subscriber server get its time from the publisher server. To verify the NTP status of the publisher server, log into the Command Line Interface on the publisher server and enter the following command: **utils ntp status**	For more information, see the Command I Reference Guide for Cisco Unified Solution release, available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products **Caution** If the publisher server fails to synchronize server, installation of a subscriber server c
Step 5	Record the network interface card (NIC) speed and duplex settings of the switch port that connects to the new server.	Enable PortFast on all switch ports that are Cisco servers. With PortFast enabled, the immediately brings a port from the blocki the forwarding state by eliminating the for [the amount of time that a port waits befor from its Spanning-Tree Protocol (STP) lea listening states to the forwarding state].
Step 6	Record the configurations settings for each server that you plan to install.	To record your configuration settings, see Information for Installation section.
Step 7	Download the signed .iso file of required Unity Connection version from Cisco.com.Upload it on a data store or burn a disk image of the downloaded software.	Download from the given link: https://software.cisco.com/download/navigator.html?mdfid=

Creating a Virtual Machine

To download the OVA template for creating virtual machines, open the following link, select Unity Connection Software, and then select the appropriate release number:

https://software.cisco.com/download/type.html?mdfid=283062758&flowid=45673.

Procedure

Step 1 To deploy the OVA template in a supported VMware client, from the File menu, select Deploy OVA template.
Step 2 Next, browse the OVA template from the URL or file location on the system.
Step 3 Follow on-screen instructions to create the virtual machine.

Changing the Boot Order of Virtual Machine

The virtual machine boot into the BIOS menu.

Procedure

Step 1 In VMware client, power off the virtual machine that has the deployed OVA template.
Step 2 In the left pane of VMware client, right-click the name of the virtual machine, and select **Edit Settings**.
Step 3 In the Virtual Machine Properties dialog box, select the **Options** tab.
Step 4 In the Settings column, from the Advanced menu, select **Boot Options**.
Step 5 In the Force BIOS Setup, check the **The next time the virtual machine boots, force entry into the BIOS setup screen** check box.
Step 6 Select **OK** to close the Virtual Machine Properties dialog box.
Step 7 Power on the virtual machine.
Step 8 Navigate to the Boot menu and change the boot device order so the CD-ROM device is listed first and the Hard Drive device is listed second.
Step 9 Save the change and exit BIOS setup.

Changing Reservation on Virtual Machines Running with E7 or E5 Processors

The CPU reservations are now included in OVAs, which are based on the Xeon 7500 processor. For E7 processors and certain E5 processors, the CPU reservations are higher than available cycles on 1 virtual CPU. In such cases, the administrator needs to change the reservation number of the virtual machine manually using the steps mentioned in Changing Reservation Numbers

Additionally, based on the lab tests, we see that the 2.4 GHz reservation on E7 or E5 processor has the same performance as a 2.53 GHz Xeon 7500 processor.

For more information see the docwiki available at http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware.

Changing the Reservation Numbers

Procedure

Step 1 In VMware vSphere Client, select the host on which virtual machine is created.

Step 2 Click the **Summary** tab, under CPU, note the available CPU cycles for 1 virtual CPU in GHz.

Step 3 Power off the virtual machine on which you deployed the OVA template

Step 4 In the left pane of vSphere Client, right-click the name of the virtual machine and select **Edit Settings**.

Step 5 In the Virtual Machine Properties dialog box, select the **Resources** tab.

Step 6 In the Settings column, select **CPU**.

Step 7 Under Resource Allocation, enter the new reservation value in the Reservation textbox. The new reservation value is calculated as the number of CPUsX2.4GHz (for E5440 processor) and the number of CPUs multiplied by the 1 virtual CPU cycles in GHz (from step 2) (for E7 processor).

Step 8 Click **OK** to close the Virtual Machine Properties dialog box.

Step 9 Power ON the virtual machine.

Verifying DNS Settings

Procedure

Step 1 Login to command prompt.

Step 2 To ping each server by its DNS name, enter **ping***DNS_name*.

Step 3 To look up each server by IP address, enter **nslookup***IP_address*.

Gathering Information for Installation

Use the Table 1-2 to record the information about your server. Gather this information for a single Unity Connection server or for both the servers in a Unity Connection cluster. You should make copies of this table and record your entries for each server in a separate table.

Table 2: Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Inst
Time Zone: _____	Sets the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your server. **Caution** In a cluster, you must set the subscriber server to the same time zone as the publisher server.	Yes, using the CLI command CLI > **set timezone**
MTU Size: _____	Sets the largest packet, in bytes, that is transmitted by this host on the network. By default, MTU is set to the size defined in the operating system. Selecting a different packet size would be more prevalent where a VPN or IPsec tunnel is used with a custom packet size. Web access over VPN can cause web pages not to load because of an improper MTU configuration. The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network. **Note** In clustered server pairs, the MTU setting must be the same on both servers	Yes, using the CLI command CLI > **set network mtu**

Configuration Setting	Description	Can Setting Be Changed After I
Hostname and IP addresses: DHCP (Yes/No): _____ If DHCP is **No**: Hostname: _____ IP Address: _____ IP Mask: _____ Gateway (GW) Address:_____	Sets whether to use DHCP to automatically configure the network settings on your server. If you select **No**, you must enter a hostname, IP address, IP address mask, and the gateway IP address. The hostname can contain up to 50 alphanumeric characters, hyphens, underscores, and period. The first character cannot be a hyphen. We recommend you use static Dynamic Host Control Protocol (DHCP) host configuration to ensure the DHCP server always provides the same IP address settings to the server **Note** If you do not have a gateway, you must still set this field to 255.255.255.255. Not specifying a gateway may limit you to only being able to communicate with devices on your subnet. **Caution** Make sure not to use ciscounity in the hostname of the server else enterprise replication gets broken.	Yes, using the CLI command CLI > **set network dhcp** CLI > **set network gateway** CLI > **set network ip eth0**
Domain Name Server: DNS: (Yes/No): _____ If DNS is **Yes**: Domain: _____ DNS Primary: _____ DNS Secondary: _____	Sets whether a DNS server resolves a hostname and IP address. **Note** Unity Connection enables the use of a domain name server to locate other Cisco Unity servers and devices. This is necessary when configuring digital networking and clustered server pairs. We recommend you to configure a secondary DNS server to avoid any loss of connectivity or service.	Yes, using the CLI commands CLI > **set network dns** CLI > **set network domain**

Configuration Setting	Description	Can Setting Be Changed After Inst
Administrator Account Credentials: Login: _____ Password: _____	Sets the administrator credentials for secure shell access to the CLI and for logging into Cisco Unified Communications Operating System and Disaster Recovery System. The administrator account should be shared only with installers and engineers who have a thorough understanding and are responsible for platform administration and upgrades, and backup and restore operations. **Note** Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Login: No. Password: yes, using the CLI comm CLI > **set password user admin** **Note** You can create additional administ accounts after installation.
Certificate Information: Organization: _____ Unit: _____ Location: _____ State: _____ Country: _____	Sets information used by the server to generate certificate signing requests (CSRs) that are used to obtain third-party certificates. **Tip** To enter more than one business 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. For location, you can enter any setting that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, using the CLI command CLI > **set web-security**
Cluster: First server in cluster (Yes/No): ____ If First server is **No**: Publisher hostname: _____ Publisher IP address: _____ Publisher security password: _____	First server refers to the publisher server. During the installation of second or subscriber server, enter the details of the first server.	

Configuration Setting	Description	Can Setting Be Changed After I
NTP Servers: NTP Server 1: _____ NTP Server 2: _____ NTP Server 3: _____ NTP Server 4: _____ NTP Server 5: _____	Sets the hostname or IP address of one or more network time protocol (NTP) servers that synchronizes with your Unity Connection server. The NTP service ensures that the time synchronized is accurate for date/timestamps of messages, reports, and various tools, such as logs and traces. All Unity Connection servers require an external NTP source that are accessible during installation. The source can be a corporate head-end router synchronized with a public NTP time server or it can be the public NTP time server itself. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v6. The NTP server that you specify for the publisher server is automatically applied for the subscriber server.	Yes, using Cisco Unified Opera Administration: **Settings > NTP Servers** Using the CLI command CLI > using the CLI command
Security Password	Sets the password used by a subscriber server to communicate with a publisher server. The security password is also used by the Disaster Recovery System to encrypt backups. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.	Yes, using the CLI command CLI > **set password user secu** **Caution** If you are changing the security a clustered server pair you mus security password on both serve both servers. For more informa description of this command in t Line Interface Reference Guide Unified Solutions.

Configuration Setting	Description	Can Setting Be Changed After Inst
SMTP Server	Sets the hostname or IP address for the SMTP server that is used for outbound e-mail, intrasite links, Voice Profile for Internet Mail (VPIM), and HTTPS networking. The hostname can contain alphanumeric characters, hyphens, or periods but it must start with an alphanumeric character. **Note** You must specify an SMTP server if you plan to use electronic notification.	Yes, using the CLI command: CLI > **set smtp**
Application Account Credentials: Login: _____ Password: _____	Sets the default credentials for the Unity Connection applications, including Cisco Unity Connection Administration and Cisco Unity Connection Serviceability.	Yes, using Cisco Unity Connection Administration and the CLI comm CLI > **utils cuc reset password**

Installation Scenarios

Table 3: Installation Scenarios

Installation Scenarios	Installation Method
Standalone Deployment	Standard • Installing the Publisher Server • Verifying the Installation Unattended • Generating Answer File for Unattended Installation • Installing the Publisher Server • Verifying the Installation

Installation Scenarios	Installation Method
Cluster Deployment	Standard • Installing the Publisher Server • Configuring Subscriber Server on the Publisher Server • Installing the Subscriber Server • Verifying the Installation Unattended • Generating Answer File for Unattended Installation • Installing the Publisher Server • Configuring Subscriber Server on the Publisher Server • Installing the Subscriber Server • Verifying the Installation

Installation Tasks

Depending on the type of installation scenario, you need to perform the following tasks to install the Unity Connection software:

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see Table 1-4.

Table 4: Installation Wizard Navigation

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

Installing the Publisher Server

While installing a Unity Connection server, you are prompted to enter different configuration information. Refer the table mentioned in the Gathering Information for Installation section wherever applicable.

Procedure

Step 1 Prepare the virtual machine to install Unity Connection:

a) Select Edit virtual machine settings to select the ISO image from CD/DVD drive using client device or from data store.

b) Navigate to the Console tab. A screen prompting you to check the integrity of the DVD appears.

c) Select **Yes** to perform the media check or **Skip** to move to the next step.

Note
If you select media check and it fails, either download another copy from Cisco.com or obtain another DVD directly from Cisco.

d) After performing the hardware check, you get a prompt to restart the system. You need to select **Yes** to continue installation. After the system restarts, the Product Deployment Selection window displays.

Step 2 In the Product Deployment Selection window, select **OK** to install Cisco Unity Connection. Then Proceed with Install window appears.

Step 3 In the Proceed with Install window, select **Yes** to continue the installation.

Caution
If you select **Yes** on the **Proceed with Install** window, all existing data on your hard drive gets overwritten and destroyed.

The Platform Installation Wizard window appears.

Step 4 In the Platform Installation Wizard window, select the applicable option:

- If you want to perform a standard installation, select **Proceed**, and continue with this procedure.
- *(Applicable to Unity Connection 14SU1 and later releases)* If you want to Import data from SFTP server during fresh install, select **Import** and continue.
- If you want to perform an unattended installation, select **Skip**. Connect the answer file image on a virtual floppy diskette and select **Continue**. The installation wizard reads the configuration information during the installation process and then follow the steps mentioned in the Post-Installation Tasks section.

Step 5 a) If you select **Proceed** in the previous window, the Apply Patch window appears:

- Select Yes to upgrade to a later Service Release of the software during installation and follow the process mentioned in the Applying a Patch section.

  Note
  This option is not applicable to Install with Data import installation method.

- Select No to skip this step and the Basic Install window appears.

b) If you select **Import** in the previous window, the Import Upgrade Configuration Information window appears. It explains the format of entering SFTP server and Export Directory. Select **OK**. The Timezone Configuration window appears. Continue with **Step-7**.

Step 6 In the Basic Install window, select **Continue** to install the software version or configure the pre- installed software. The Timezone Configuration window appears.

Step 7 In the Timezone Configuration window, select the appropriate time zone for the server and then select **OK**. The Auto Negotiation Configuration window appears.

Caution
In a cluster, the subscriber server must be configured to use the same time zone as the publisher server. The replication do not work if the timezone is not same.

Step 8 In the Auto Negotiation Configuration window, select **Continue**. The MTU Configuration window appears.

Step 9 In the MTU Configuration window, select the applicable option:

- Select **No** to accept the default value (1500 bytes).
- Select **Yes** to change the MTU size, enter the new MTU size, and select **OK.**

Caution
If you configure the MTU size incorrectly, your network performance can be affected.

The DHCP Configuration window appears.

Step 10 In the DHCP Configuration window, select the applicable option:

- Select **Yes** to use DHCP server that is configured in your network.The network restarts and the Administrator Login Configuration window appears.
- Select **No** to configure a static IP address for the server and continue with this procedure. The Static Network Configuration window appears.

Step 11 In the Static Network Configuration window, enter the static network configuration information.

The DNS Client Configuration window displays.

Step 12 To enable DNS, select **Yes**, enter the DNS client information and select **OK**.

The network restarts using the new configuration information.

Step 13 a) If **Import** option is selected in **Step-4** then Software Location of Data to import window will display. In this window, enter the following information.

Field	Description
Remote Server Name or IP	The Secure FTP (SFTP) server that will store the source cluster's exported data.
Export Data Directory	Directory path on the server containing export data.
Remote Server Login ID	Allow for data retrieval of the remote SFTP server.
Remote Server Password	Contains alphanumeric characters, hyphens, and underscores

The Certificate Information window appears.

b) If **Import** option is not selected in **Step-4** then enter the administrator login and password. The Certificate Information window appears.

Step 14 Enter your certificate signing request information and select **OK**.

The First Node Configuration window displays.

Step 15 In the First Node Configuration window, select the applicable option:

- Select **Yes** to configure this server as the publisher server or as a standalone server and continue this procedure. The Network Time Protocol Client Configuration window appears.
- Select **No** to configure this server as the subscriber server.

Step 16 In the Network Time Protocol Client Configuration window, enter the hostname or IP address of the NTP server(s) and select Proceed.

Note
Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher server. However, you can configure multiple NTP servers based on your requirements.

Step 17

a) If **Import** option is not selected in **Step-4** then Security Configuration window appears.In the Security Configuration window, enter the security password.

Note
The system uses this password to authorize communications between the publisher and subscriber servers; you must ensure this password is identical on the two servers.

The SMTP Host Configuration window appears.

b) If **Import** option is selected in **Step-4** then SMTP Host Configuration window appears after selecting Proceed on the Network Time Protocol Client Configuration window.

Step 18 In the SMTP Host Configuration window:

a) Select **Yes** to configure an SMTP server and enter the SMTP server name or IP address.
b) Select **OK**. The Application User Configuration window appears.

Note
You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later using the platform GUI or the command line interface.

If **Import** option is selected in **Step-4**, then Platform Configuration Confirmation window appears after selecting OK on the SMTP Host Configuration window. Continue with **Step-20**.

Step 19 In the Application User Configuration window:

a) Enter the Application User name and password and confirm the password by entering it again.

Note
Do not use the system application name as the Application User name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database. The system application names are operator, replication, undeliverablemessagesmailbox, and Unity Connection.

b) Select **OK**. The Platform Configuration Confirmation window appears.

Step 20 In the Platform Configuration Confirmation window, select **OK** to continue the installation. The system installs and configures the software.

Step 21 When the installation process completes, you are prompted to log in using the Administrator account and password.

Configuring Subscriber Server on the Publisher Server

Procedure

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand System Settings and select Cluster.

Step 3 On the Find and List Servers page, select Add New.

Step 4 On the New Server Configuration page, in the Hostname or IP Address field, enter the hostname or IP address of the second server in the cluster.

Step 5 *(Optional)* In the MAC Address field, enter the MAC address of the second server.

Step 6 In the Description field, enter **a** description for the second server and select **Save**.

Note
Above mentioned steps are applicable to:

- Unity Connection 14 release.
- If **Import** option is not selected, while installation for Unity Connection 14SU1 and later releases.
- If **Import** option is selected only for publisher node, while installing Unity Connection 14SU1 and later releases.This is the case network migration in which data is exported and imported on publisher node only and subscriber node is freshly installed.

Installing the Subscriber Server

Note In case of **Install with Data Import** installation method, you can fresh install the subscriber node or you can import the subscriber node using Import option.

For importing the subscriber node, select the Import option in Platform Installation Wizard window and follow the steps of importing publisher server until the First Node Configuration window appears.Then continue the following procedure.

To fresh install the subscriber server, follow the steps of installing publisher server until the First Node Configuration window appears and then continue the following procedure.

While installing a Unity Connection server, you are prompted to enter different configuration information. Refer the table mentioned in the Gathering Information for Installation section wherever applicable.

Procedure

Step 1 In the Console tab, on the First Node Configuration window, select No to continue the installation of the subscriber server and select **OK**.

The **Network Connectivity Test Configuration** window displays.

Step 2 During installation of a subscriber server, the system checks to ensure that the subscriber server can connect to the publisher server.

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

The **First Node Access Configuration** window displays.

Step 3 Enter the connectivity information for the publisher server and select **OK**.

The system checks for network connectivity.

If you select to pause the system after the system successfully verifies network connectivity, the Successful Cisco Unity Connection to First Node window displays. Select **Continue**.

Note
If the network connectivity test fails, the system stops and allows you to go back and re-enter the parameter information.

The **SMTP Host Configuration** window displays.

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

The **Platform Configuration Confirmation** window displays.

Step 5 Select **OK** to start installing the software.

Step 6 When the installation process completes, you are prompted to log in using the Administrator account and password.

Note
After installing publisher and subscriber nodes, complete the post-installation tasks that are listed in the Post-Installation Tasks, on page 29. In case of Install with Data Import option, complete the post-migration tasks listed in the Post-Migration Tasks section.

Generating Answer File for Unattended Installation

You can generate answer files using Cisco Unified Communications Answer File Generator web application. To use the answer file during installation, you need to save the answer file to the root directory of a floppy diskette, browse to the file during installation, and leave the installation to complete.

In case of Unity Connection cluster:

- You need to generate separate answer files for publisher and subscriber servers.
- You are not required to enter details of the publisher server manually on the subscriber server during subscriber server installation.

Note The Cisco Unified Communications Answer File Generator supports Internet Explorer version 11.0 or higher and Mozilla version 28.0 or higher.

Task List for Unattended Installation

You need to perform the following tasks to generate answer file and create floppy image for unattended installation.

1. Generate and download answer files that includes the platformConfig.xml files for both the publisher and the subscriber server. For more information on how to generate answer files, see Generating and Downloading Answer File.
2. After generating the answer files, create a floppy image. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739.
3. Deploy and configure the servers in the cluster, publisher and subscriber. For more information, see the Configuring the Publisher Server and Configuring the Subscriber Server section.
4. To install the publisher and subscriber server, see the Installing Publisher Server and Installing the Subscriber Server section.

Generating and Downloading Answer File

Procedure

Step 1 Log in to the Unity Connection Answer File Generator application. The answer file can be generated using the following link: http://www.cisco.com/web/cuc_afg/index.html.

Step 2 Enter details in the Clusterwide Configuration section.

Note
(Applicable to Unity Connection 14SU1 and later releases) You can select option **Configure Software Location of Data to Import** for using **Install with Data Import** installation method. Enter details of Remote Server and Export Data Directory.

Step 3 Enter details for the primary node in the Primary Node Configuration section.

Step 4 (Optional) If you want to enable Dynamic Cluster Configuration, enter a value in the Dynamic-cluster-config-timer field.

Note
Step 4 is mandatory when you are using Dynamic-cluster-configuration process for Touchless installation.

Step 5 Enter details for the secondary node in the Secondary Node Configuration section.

Step 6 In the List of Secondary Nodes list box, select Add Secondary Node. The node that you add as secondary node appears in this list box.

Step 7 Click Generate Answer Files. A dialog box appears showing the details for the primary node, the secondary node, and the clusterConfig file.

Step 8 In the Communications Answer File Generator dialog box, follow the download instructions, and then click the Download File button to download the answer files to your computer.

Configuring the Publisher Server

Procedure

Step 1 Log in to the virtual machine to start the cluster installation.

Step 2 From the VM menu, select Edit settings to mount the floppy image that you have created from the Answer File Generator tool. The Virtual Machine Properties dialog box appears.

Step 3 From the available hardware list, select Floppy drive 1.

Step 4 In the Device Type section, select Use the existing floppy image in the database, and then click Browse to navigate to the floppy image.

Step 5 Click OK. The floppy image is attached.

Step 6 Select the CD/DVD Drive 1 > Connect to ISO image on local disk option from the toolbar and select CD/DVD Drive1 > Connect to ISO image on a datastore, navigate to the data store to select the ISO image, and click OK. The ISO image is attached and the installation starts.

Step 7 (Optional) If you want to test the media before the installation, click OK in the Disc Found message box, or select Skip to skip testing the media before the installation. The installation proceeds without any manual intervention. The publisher is installed and the subscribers is added to the publisher.

Configuring the Subscriber Server

Procedure

Step 1 You can install the subscriber only after the publisher is installed.(Applicable to only unattended installation, not valid for Touchless install).

Step 2 Perform Step 1 to Step 6 of the Configuring the Publisher Server.

Touchless Installation for Virtual Machine

Touchless installation is an enhancement of the existing unattended installation, which promotes simplified cluster installation. In unattended installation, you first install Unity Connection on the publisher server using answer file, add the subscriber server to the Cluster page of the publisher server, and then start the installation of subscriber server. However, in Touchless installation, you are not required to manually enter the details of the subscriber server on the publisher server. The subscriber details are automatically updated through clusterConfig.xml file or dynamic-cluster-configuration option in the AFG tool, which minimizes the need for intervention and scheduling during the deployment of a new cluster.

Methods for Touchless Installation

You can use either of the following two methods for Touchless installation:

- Predefined Cluster Configurations (AFG Process)
- Automatic Sequencing of Touchless server (Subscriber-Dynamic-Cluster configuration).

  Predefined Cluster Configurations (AFG Process)

In this method of installation, the Answer File Generator (AFG) tool generates the clusterConfig.xml file along with the existing platformConfig.xml file for both the publisher and subscriber servers. If you specify the details of the subscriber server in the AFG tool, those details are included in the clusterConfig.xml file. After the publisher server is installed, it reads the clusterConfig.xml file and if the publisher server finds the subscriber server, it adds the subscriber server to its processnode table. Adding the subscriber server to the processnode table eliminates the need to wait for the publisher server to finish its installation, and then manually add the subscriber server on the server page.Thus, the entire installation process occurs automatically.

Automatic Sequencing of Touchless Server (dynamic-cluster-configuration)

In automatic sequencing feature, subscriber gets configured dynamically along with the publisher during the installation. To use this functionality, enable the dynamic-cluster-configuration option in the AFG tool or use the command line interface (CLI) command on the publisher server. To use CLI to enable dynamic-configuration functionality, see (Optional) Enabling Dynamic-Cluster-Configuration Using CLI. There is no clusterconfig.xml file in this process of Touchless install.You need to enable the Dynamic Cluster Config Timer (1-24 hours) and start the installation on both the servers at the same time. The number of hours is the duration for which subscriber waits for publisher to receive the subscriber entry in the processnode table.

Task List for Touchless Installation

You need to perform the following tasks to generate answer files and create floppy image for Touchless installation.

1. Generate and download answer files that includes the platformConfig.xml files for both the publisher and the subscriber server and clusterconfig.xml file (only for AFG Process). For more information on how to generate answer files, see Generating and Downloading Answer File.

Note In case you are using dynamic-cluster-configuration method of installation, then you just need to enable dynamic-cluster-configuration option in the AFG tool and follow the step1.

2. After generating the answer files, create a floppy image. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739.
3. Deploy and configure the servers in the cluster, publisher and subscriber. For more information, see the Configuring Publisher Server and Configuring Subscriber Server section.
4. To install the publisher server, see the Installing Publisher Server section for cluster deployment.
5. The installation of subscriber continues if:

   - You enable the dynamic-cluster-configuration timer.
   - The clusterConfig.xml files are present.

(Optional)

(Optional) Enabling Dynamic-Cluster-Configuration Using CLI

Procedure

	Command or Action	Purpose
Step 1	You can enable Dynamic-Cluster-Configuration through the CLI for up to an hour using the command: set network cluster subscriber dynamic-cluster-config {default | no. of hours}. For more information, see the "Set Command" chapter of *Command Line Interface Guide for Cisco Unified Communications Solutions* available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html	
Step 2	Add the new cluster subscriber through the CLI in the following format: set network cluster subscriber details <servertype> <hostname> <ip> <domainname>.	
Step 3	You can use show network cluster CLI to check the entries in the processnode table. For more information, see "Show Command" chapter of *Command Line Interface Guide for Cisco Unified Communications Solutions* available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html	

Automated Installation using vApp properties and VMware OVF Tool

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

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

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

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

Task List for Manual Installation using vApp Options

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

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

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

Procedure

Step 1 Deploy skip-install OVA after obtaining it from **My Cisco Entitlements**.

Step 2 From VMware Embedded Host Client or vCenter Server, deploy OVA using the **Browse** button or enter a URL to download and install the OVA package from the Internet.

Step 3 Enter the required Unity Connection configurations, skip-install OVA, VMware Embedded Host Client, or vCenter for each node in the cluster.

Step 4 To perform touchless install on cluster, make sure to check the **Dynamic Cluster Config Enable** check box in user interface of the Unity Connection publisher, and enter a value between 1-24 in the **Dynamic cluster Config Timer** field in case of cluster installation. (OR) Add your subscriber node manually from the Unity Connection user interface of the publisher, after the publisher node installation completes.

Step 5 For installation using Fresh Install with Data Import, follow the instructions in Install with Data Import, on page 3 section.

Step 6 Once the OVA image is deployed successfully into the virtual machine, power on the Virtual Machine.You will observe that the installation is in process. Repeat step 3 for subscriber node in the cluster by providing the IP Address and Host Name of the Unity Connection publisher node. Subscriber node can be installed parallelly by opening VMware Embedded Host Client.

Task List for Touchless Installation using VM Tools

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

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

Before you begin

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

The Cisco VM Builder tool (VMware wrapper tool) and the dependent tool will be bundled and provided as .rpm file (platform-skip-install-ovftool-1.0.0.0-1.x86_64.rpm) or as a g-zipped tar file/tarball (platform-skip-install-ovftool_v1.0.tar.gz.) See the ReadMe guide for instructions on how to install .rpm/tar.

Procedure

Step 1 Install the Cisco VM Builder tool from **My Cisco Entitlements** on Linux based SFTP server.

Step 2 Copy the Unity Connection OVA image from **My Cisco Entitlements** to the same server.

Step 3 Using the Cisco VM Builder tool pass the required Unity Connection configurations, skip-install OVA and VMware Embedded Host Client or vCenter for each node in the cluster based on the type of Install. Install can be Fresh Install or Fresh Install with Data Import. Configurations differ for the publisher and subscriber nodes. Use the "vmbuilder--help" option to know more about the parameters to be used.

Step 4 To perform cluster installation, make sure to pass the Dynamic Cluster Config Enable parameter as True and enter a value between 1-24, in the Dynamic cluster Config Timer in the Cisco VM Builder tool of the Unity Connection publisher. Set the values of these parameters as: **guest.dynamic_cluster_config=True** and **guest.cluster_config_timer=24**. (OR) Add your subscriber node manually from the Unity Connection user interface of the publisher, after the publisher node installation completes.

Step 5 The Cisco VM Builder tool validates the configuration values, deploys the OVA in the VMware Embedded Host Client or vCenter Server, automatically powers on the node, and starts the installation. See the "**vmbuilder--help**" option to know more about the mandatory parameters and other restrictions.

Step 6 Repeat **Step-3** for subscriber node in the cluster. Subscriber node can be installed parallelly by opening another SSH connection.

Applying a Patch

You must obtain the appropriate upgrade file from Cisco.com before you can upgrade during installation. To apply a patch, select **Yes** in the Apply a Patch window that appears during the installation of publisher or subscriber server. The installation wizard installs the software version on the DVD first and then restarts the system.

Note You can upgrade to any supported higher release if you have a full patch of the release not an Engineering Special (ES).

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

Procedure

Step 1 If you select **Yes** in the Apply a Patch window, the Install Upgrade Retrieval Mechanism Configuration window appears.

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

- **SFTP**—Retrieves the upgrade file from a remote server using the Secure File Transfer Protocol (SFTP). Skip to the Upgrading from a Remote Server.

- **FTP**—Retrieves the upgrade file from a remote server using File Transfer Protocol (FTP). Skip to the Upgrading from a Remote Server.
- **LOCAL**—Retrieves the upgrade file from a local DVD. Continue with the Upgrading from a Local Disk.

Upgrading from a Remote Server

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

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

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

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

Procedure

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

Step 2 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) using automatic negotiation. You can change this setting after installation.

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

- To enable automatic negotiation, select **Yes**.

  The MTU Configuration window displays. Continue with Step 4.

- To disable automatic negotiation, select **No**. The NIC Speed and Duplex Configuration window displays. Continue with Step 3.

Step 3 If you select to disable automatic negotiation, manually select the appropriate NIC speed and duplex settings now and select **OK** to continue.

The MTU Configuration window displays.

Step 4 In the MTU Configuration window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that is transmitted by this host on the network. If you are unsure of the MTU setting for your network, use the default value.

Caution
If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), select **No**.
- To change the MTU size from the operating system default, select **Yes**, enter the new MTU size, and select **OK**.

The DHCP Configuration window displays.

Step 5 For network configuration, you can select to either set up static network IP addresses for the Unity Connection server and gateway or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended.

- If you have a DHCP server that is configured in your network and want to use DHCP, select Yes. The installation process attempts to verify network connectivity.
- If you want to configure static IP addresses for the server, select No. The Static Network Configuration window displays.

Step 6 If you select not to use DHCP, enter your static network configuration values and select OK.

The DNS Client Configuration window displays.

Step 7 To enable DNS, select Yes, enter the DNS client information and select OK.

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

Step 8 Enter the location and login information for the remote file server. The system connects to the remote server and retrieves a list of available upgrade patches.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path that starts with a drive letter (for example, C:).

The Install Upgrade Patch Selection window displays.

Step 9 Select the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system with the upgraded software version running.

After the system restarts, the Pre-existing Configuration Information window displays.

Step 10 To continue the installation, select **Proceed**.

The Platform Installation Wizard window displays.

Step 11 To continue the installation, select **Proceed** or select **Cancel** to stop the installation.

If you select **Proceed**, the Apply Patch window displays. Continue with Step 12.

If you select **Cancel**, the system halts, and you can safely power down the server.

Step 12 When the Apply Patch window displays, select **No,** the "Basic Install" window appears.

Step 13 Select **Continue** in the window to install the software version on the DVD or configure the pre- installed software and move to Step 7 of the Installing the Publisher Server section.

Upgrading from a Local Disk

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

Procedure

Step 1 When the Local Patch Configuration window displays, enter the patch directory and patch name, if required, and select **OK**.

The Install Upgrade Patch Selection Validation window displays.

Step 2 The window displays the patch file that is available on the DVD. To update the system with this patch, select **Continue**.

Step 3 Select the upgrade patch to install. The system installs the patch, then restarts the system with the upgraded software version running.

After the system restarts, the Preexisting Configuration Information window displays.

Step 4 To continue the installation, select **Proceed**.

The Platform Installation Wizard window displays.

Step 5 To continue the installation, select **Proceed** or select **Cancel** to stop the installation.

If you select **Proceed**, the Apply Patch window displays. Continue with Step 6.

If you select **Cancel**, the system halts, and you can safely power down the server.

Step 6 When the Apply Patch window displays, select **No,** the "Basic Install" window appears.

Step 7 Select **Continue** in the window to install the software version on the DVD or configure the pre- installed software and move to Step 7 of the Installing the Publisher Server section.

Verifying the Installation

After the installation application has finished, the new server displays its hostname and the administration account login prompt.

Procedure

Step 1 Log in with the administration account user name and password.

The server opens a command line interface.

Step 2 Verify that server network services are running:

a) At the CLI prompt, enter the command **utils service list.**

It might take a few minutes for all services to start completely. During this time, you might notice that services might be listed as [Starting].

b) Repeat the **utils service list** command until all network services are listed as [Started].

In particular, the Cisco Tomcat service must be started before you can proceed to the next verification step.

Step 3 Verify the server details:

a) Open a web browser on a personal computer that has network access to the server. Unity Connection supports different web browsers, such as Microsoft Internet Explorer and Mozilla Firefox.
b) In the web browser, enter the URL "https://<*publisher_ip_address*>/cmplatform".
c) Login to Cisco Unified OS Administration using the *administrator* user name and password specified during the installation.
d) Select **Show > System** from the toolbar to display the system status page, showing the current date, uptime, software level, along with the CPU and memory usage.
e) Use the **Show** menu to check:

- **Cluster: displays the IP address, hostname, alias, server type, and database replication status of the single server or both the server in case of cluster.**
- **Hardware**: platform type, serial number, hardware, and other options
- **Network**: current network interface configuration, status, and packets
- **Software**: current active and inactive software partitions

Step 4 Verify the server status:

a) In the web browser, enter the URL "https://<*publisher_ip_address*>/cuadmin".
b) The Cisco Unity Connection Administration window opens. Select Cisco Unity Connection Serviceability from the navigation pane. Login using the *application* user name and password specified during the installation.
c) Select Tools > Cluster Management. It lists the server status of either single server or both the servers in case of cluster. For a standalone server deployment, the server shows Primary status whereas in case of cluster, one of the server shows Primary status and the other shows Secondary status.

Cisco Unity Connection Survivable Remote Site Voicemail Installation

You install a Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) server by converting a standalone Unity Connection server with the CLI command

utils cuc activate CUSRSV

Warning After installing Unity Connection SRSV, you can not revert to a standalone Unity Connection server.

Caution All the existing Unity Connection configurations are lost after running the conversion.

Note The unrestricted version of Unity Connection SRSV works only with the unrestricted version of Unity Connection (central) server.

Post-Installation Tasks

After installing Unity Connection on your server, you should perform the following additional tasks before configuring the system for your application:

- Obtain the licenses for the Unity Connection server. For this, you must register the product with Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite.

  For more information, see the Managing Licenses chapter.

- (Optional) Change the application passwords.

  You can change the passwords using either the Cisco Unity Connection Administration web application, or you can log into the server and run the CLI command

  utils cuc reset password

- If you require additional languages, install them.

  For details, see the Adding or Removing Unity Connection Languages section.

- Install the Cisco Unified Real-Time Monitoring Tool.

  You can use Cisco Unified Real-Time Monitoring Tool to monitor system health, and view and collect logs. For more information on RTMT, see the Cisco Unified Real-Time Monitoring Tool Administration Guide Release at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

  (Optional): You can configure RTMT to send alert notifications through emails to the specified email address. For more information on enabling email alert, see the Enable email alerts section of the Cisco Unified Real-Time Monitoring Tool Administration Guide.

- Activate Unity Connection feature services.

  For service activation requirements, see the *Cisco Unified Serviceability Administration Guide Release 14 at* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/serv_administration/guide/b_14cucservag.html

- Configure the backup settings. For more information, see the Backing Up and Restoring Cisco Unity Connection Components chapter.

Post-Migration Tasks

Network Migration

After successful **Install with Data Import** in case of **Network Migration**, perform some additional steps as described below:

1. Obtain the Licenses for the new Unity Connection server. For configuration of licenses, see the Managing Licenses chapter.

Note Make sure to de-register the node from which export is performed to free the license consumption and then proceed for registration of new imported node.

2. If Unity Connection on source release has IPsec configured using a certificate-based authentication, then you must reconfigure the IPsec policy with a CA-signed certificate after successful installation on new Unity Connection Server. For more information, see the section Upgrade Considerations with FIPS Mode, on page 51.

3. If there is any change in certificates on new Unity connection server then regenerate and upload certificates on appropriate paths on new Unity Connection server. Some examples are given below:

   - If Unity Connection on source release has Secure SIP call configured using SIP Integration then after successful installation, generate and upload RSA based Tomcat certificates on new Unity Connection server. To learn how to regenerate certificates, see section Settings for RSA Key Based certificates of *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.
   - If Unity Connection on source release uses tomcat-ECDSA certificates (self signed and third party) for next generation security then after successful installation generate and upload tomcat-ECDSA certificates on new Unity Connection server.To learn how to regenerate certificates, see section Settings for EC Key Based certificates of *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.

4. For proper functioning of SAML SSO perform below steps:

   - Update the Metadata files of new Unity Connection server for SAML on IdP.
   - Update IdP Metadata file on new Unity Connection server.

   For more information, see *Quick Start Guide for SAML SSO Access* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/quick_start/guide/b_14cucqssamlsso/m_samlssochapter.html.

5. Update the new Unity Connection server's FQDN and IP in required telephony configurations on **Cisco Unified Communications Manager** side. For more information, see *System Configuration Guide for Cisco Unified Communications Manager* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

6. You must reinstall the set of required locales that are compatible with the new Unity Connection version.

7. Changes done by COP files installed on previous releases does not carry forward with migration and therefore COP files installed on previous release needs to be installed again. After successful migration you must manually install that COP file on new Unity Connection server.

8. If you want to change Unity Connection SMTP Domain Name, follow steps mentioned in https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/117237-technote-uc-00.html.

9. Default Partition Name does not change during Migration, hence if you want to change the Partition Name to new Name then, follow the steps mentioned in https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag/b_14cucsag_chapter_0111.html#ID-2420-000001e5

10. Before Migration, if the Unity Connection Cluster was onboarded to Cisco Webex Cloud-Connected UC, then post migration, first delete the cluster inside the cluster group, and then delete the cluster group on Cisco Webex Cloud-Connected UC. For more information, refer https://help.webex.com/en-us/article/nzt6c0b/Set-up-Webex-Cloud-Connected-UC-for-on-premises-devices#id_124573. Remove the Agent from all the nodes of Unity Connection Cluster using the CLI command "**utils ucmgmt agent remove**". To continue using SpeechView feature, Unity Connection Cluster should be onboarded again to Cisco Webex Cloud-Connected UC. For more information, refer "SpeechView Cisco Webex in-house transcription service" chapter of the *System Administration Guide for Cisco Unity Connection Release 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Simple Migration

After successful Simple Migration perform below additional steps:

1. Obtain the Licenses for the new Unity Connection server. For configuration of licenses, see the Managing Licenses chapter.

Note Make sure to de-register the node from which export is performed to free the license consumption and then proceed for registration of new imported node.

2. For successful working of IPSec, restart IPSec service on both the nodes of new Unity Connection server using below CLI:

```
utils ipsec restart
```

3. Changes done by COP files installed on previous releases does not carry forward with migration and therefore COP files installed on previous release needs to be installed again. After successful migration you must manually install that COP file on new Unity Connection server.

4. You must reinstall the set of required locales that are compatible with the new Unity Connection version.

5. Before Migration, if the Unity Connection Cluster was onboarded to Cisco Webex Cloud-Connected UC, then post migration, first delete the cluster inside the cluster group, and then delete the cluster group on Cisco Webex Cloud-Connected UC. For more information, refer https://help.webex.com/en-us/article/nzt6c0b/Set-up-Webex-Cloud-Connected-UC-for-on-premises-devices#id_124573. Remove the Agent from all the nodes of Unity Connection Cluster using the CLI command "**utils ucmgmt agent remove**". To continue using SpeechView feature, Unity Connection Cluster should be onboarded again to Cisco Webex Cloud-Connected UC. For more information, refer "SpeechView Cisco Webex in-house transcription service" chapter of the *System Administration Guide for Cisco Unity Connection Release 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Troubleshooting Installation Issues

Follow the steps in this section to troubleshoot issues faced during installation.

- Examine the log files if you encounter problems during installation. Use the following commands in Command Line Interface to view log files.

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

  ```
  CLI>file list install *
  ```

  To view the log file from the command line, enter

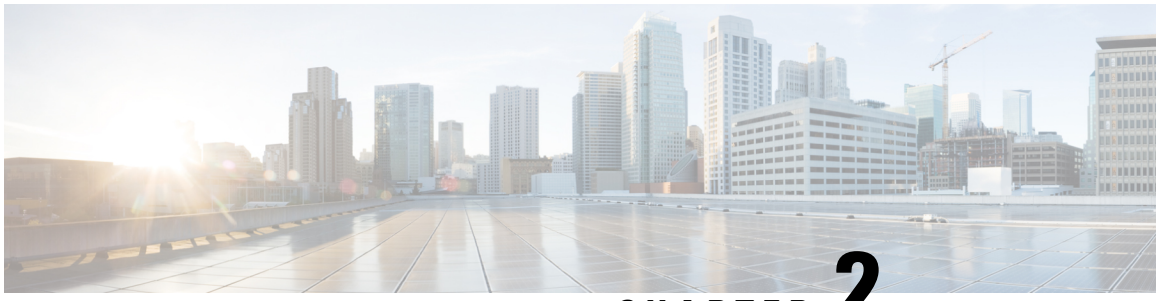
  ```
  CLI>file view install log_file
  ```

  where *log_file* is the log file name.

You can also view logs using the Cisco Unified Real-Time Monitoring Tool.

You can dump the install logs to the serial port of a virtual machine using the "Dumping Install Logs" procedure mentioned at http://docwiki.cisco.com/wiki/How_to_Dump_Install_Logs_to_the_Serial_Port_of_the_Virtual_Machine.

For more information on troubleshooting installation issues, see the *Troubleshooting Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/troubleshooting/guide/b_14cuctsg.html.



CHAPTER 2

Backing Up and Restoring Cisco Unity Connection Components

You must take the backup of Cisco Unity Connection components to avoid loosing any data or messages. The following are the tools supported for taking the backup or restoring the Unity Connection components:

- About Cobras, on page 33
- About Disaster Recovery System, on page 33
- About System Restore Tool, on page 40

About Cobras

Cisco Unified Backup and Restore Application Suite (COBRAS) is an application used to migrate data and messages. You can take the backup using Export tool and restore the backup data using Import tool.

For more information, download the latest version of COBRAS, and view the training videos and Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

About Disaster Recovery System

The Disaster Recovery System (DRS) is web application that enables you to take the full backup of Unity Connection server components to remote locations using File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP).

You can take the backup of the following Unity Connection server components:

- Unity Connection configuration database
- Mailbox messages
- User greetings and recorded names
- Other server and platform components

DRS also provides a restore wizard that enables you to restore the Unity Connection server components from a backup file stored on an FTP or SFTP server.

Note You must configure the Unity Connection server with the settings similar to the server of which backup was taken before you can restore the software components.

All the tasks related to Cisco Unified Operating System Administration web interface remain in the locked state when Disaster Recovery System backup or restore is running. This is because DRS locks the operating system platform API. All the Command Line Interface (CLI) commands continue to work except for the CLI based upgrade command since the platform API is locked.

The Disaster Recovery System contains two key components:

- Master Agent (MA)
- Local Agent (LA)

The Master Agent coordinates the backup and restore activities with Local Agents. The system automatically activates both the Master Agent and the Local Agent on all the servers in the cluster.

Disaster Recovery System backup tasks can be configured from web interface or Command Line Interface (CLI) but configuring from web interface is more preferable. For information on configuring backup tasks using CLI, see the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Components Supported for DRS Backup

You can take the backup specific Unity Connection components. The components are listed under Select Features:

- CUC: Other Unity Connection server and platform components.
- CONNECTION_GREETINGS_VOICENAMES: All user greetings and recorded names.
- CONNECTION_DATABASE: Unity Connection configuration database.
- CONNECTION_MESSAGES_<MAILBOXSTORENAME>: All messages in the named mailbox store.
- CONNECTION_HTML_NOTIFICATION: All HTML notification messages.

Note Selecting the CONNECTION_GREETINGS_VOICENAMES or CONNECTION_HTML_NOTIFICATION component automatically includes the CONNECTION_DATABASE component.

You should take the backup of all the server components when you are taking the backup for the first time, changing the backup device, upgrading the Unity Connection server to higher releases, migrating from physical server to virtual machine, or re-installing the server.

Backup Files in DRS

DRS stores the backup of all the server software components in multiple .tar files based on the component selected.

The .tar backup file includes an XML file called drfComponent.xml that contains a catalog of all the component files stored during the backup operation. When DRS performs the next backup operation, it uses the contents of this catalog to determine:

- Whether the number of.tar backup files should exceed the total number of backups you defined for the backup device.
- The .tar backup file to erase.

Caution DRS encrypts the .tar backup files using the security password configured during the installation of Unity Connection server. If you decide to change this password, perform a full DRS backup immediately. You must use the same security password on the replacement server when performing a restore

operation.

Configuring DRS Backup

Note In a cluster deployment, you need to take the backup of publisher server only

Procedure

Step 1 Set up and configure the FTP or SFTP server(s) used for storing the backups.

A number of SFTP applications, such as Free FTP and Core FTP mini SFTP server are available that can be used to store and retrieve the backups.

To configure the FTP or SFTP server, you must define the directory that stores the backup and create an account that DRS can use to store and retrieve the backups.

Note
Make sure there is enough capacity in the directory for the required number and size of backups. Keep in mind that the size of the backups increase as the organization grows.

Step 2 Configure a backup device in DRS.

Each DRS backup device consists of the backup location, the FTP or SFTP account credentials, and the total number of backups that can be stored at the backup location. When the total number of allowed backups is reached, DRS overwrites the oldest backup on the server.

Follow the given steps to configure a backup device:

- Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.
- Select Backup> Backup Device. The Backup Device window displays. Select Add New.
- Enter the backup device name, network configuration information and the number of backups to store on network directory.
- Select Save to create the backup device.

Note
Depending on the backup policy and organization, it is advisable to create multiple backup devices for redundancy. If the organization consists of multiple locations, each location should have its own set of backup devices

Caution
Do not use the same network location/directory for different backup devices. Backup files for each Unity Connection server must be stored in a directory dedicated to that server.

Step 3 Configure the backup process

After creating the backup device, you can

- Configure a backup schedule using Configuring a Backup Schedule, on page 36
- Configure a manual backup using Configuring a Manual Backup, on page 37

Configuring a Backup Schedule

You can create a different backup schedule for each backup device you created. Backup schedule can be configured to run the backup at different times. It is recommended to take multiple schedules, each stored on a different network location.

In most of the cases, you should set a schedule that performs a nightly backup during a defined maintenance window when there is the least amount of server and network traffic.

You can configure up to ten backup schedules, each has its own backup device, features, and components.

Note Disabling the schedule allows you to prevent the scheduled backups from running without deleting the schedule entirely.

To Configure a Backup Schedule for Each Backup Device in Disaster Recovery System

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> Scheduler**. The Schedule List window displays.

Step 3 On the **Schedule List** window, select **Add New** to create a new backup schedule. The Scheduler window displays.

Step 4 On the Scheduler window, the following information are mentioned to configure a schedule:

- **Schedule Name**: Specify a schedule name.
- **Select Backup Device**: Specify the backup device for which you want to create a schedule.
- **Select Features**: Specify the Unity Connection components you want to backup.
- **Starts Backup a**t: Specify the starting date and time of the schedule.
- **Frequency**: Specify the daily, weekly, or monthly cycles of the schedule.

Step 5 Select **Save** to apply the backup schedule.

Note
If you select the Set Default option in the toolbar enables you to configure the backup schedule to perform weekly backups on Tuesday through Saturday.

Configuring a Manual Backup

You can run a manual backup for all components each time you create or change the configuration of a backup device.

Note Make sure to select all the components listed for backup.

The amount of time required to complete the backup depends on the size of the database and the number of components selected for backup. The maximum time taken for backup to complete is 20 hours or it gets time out.

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> Manual Backup**. The Manual Backup window displays.

Step 3 On the Manual Backup window,

- **Select Backup Device:** Specify the backup device to be used for backup.
- **Select Features:** Specify the Unity Connection components you want to backup.

Step 4 Select **Start Backup** to start the manual backup.

DRS generates a log file for each component after completing its backup. If an error occurred, you can open the component's log file to identify the specific error.

Viewing the Backup Status

To View the Backup Status in Disaster Recovery System

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> Current Status**. The Backup Status window displays.

Step 3 The **Backup Status** window displays the current status of the components selected for backup.

Step 4 You can select Cancel Backup to cancel the backup after the backup of the current component completes.

Viewing the Backup History

To View the Backup History in Disaster Recovery System

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup> History**. The Backup History window displays.

Step 3 On the **Backup History** window you can view the backup history after running a manual backup, to ensure it completed successfully.

Step 4 You can select Cancel Backup to cancel the backup after the backup of the current component completes.

Configuring DRS Restore

In case of Unity Connection cluster, you take the backup of publisher server only. Therefore, you need to restore only on the publisher server.

To Restore the Software Components on Unity Connection

Procedure

Step 1 Install a new Unity Connection server.

The new server must be installed with exactly the same software and patches as the server being removed from service, and must be configured with the same hostname, IP address, and deployment type (standalone server or cluster pair). For example, the Disaster Recovery System does not allow a restore from version 8.5(1).1000-1 to version 8.5(2).1000-1, or from version 8.5(2).1000-1 to version 8.5(2).1000-2. (The last parts of the version number change when you install a service release or an engineering special.)

Step 2 Follow the given steps after reinstalling Unity Connection:

a) Confirm that the IP address and hostname of the server matches the IP address and hostname of the server as it was before taking the backup.

b) Confirm that the following settings match the values when taking the server backups:

- Time zone
- NTP server
- NIC speed and duplex settings
- DHCP settings
- Primary DNS settings
- SMTP hostname
- X.509 Certificate information (Organization, Unit, Location, State, and Country)

c) Confirm that the security password of the server matches the security password of the server as it was before taking the backup.

DRS encrypts the backup data using security password as the encryption key. If you change the security password of the Unity Connection server after the last backup was taken, you need to enter the old security password during the restore process.

d) If any Unity Connection languages were previously installed, reinstall the same languages on the server.

Step 3 On the new server, log in to Disaster Recovery System (DRS) and recreate the backup device used to store the backups from the server removed from service.

Step 4 Follow the given steps to run the restore operation in DRS:

a) Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

b) Run the **Restore Wizard**.

From the toolbar, select **Restore** > **Restore Wizard**.

c) Select the backup device you re-created and select **Next**.

d) Select the backup .tar file to restore the components and select **Next**.

Note
DRS time stamps each backup file enabling you to easily select the backup file to use for a restore operation.

e) Select the software components to restore and select **Next**.

f) Select the specific server to restore each component.

Additionally, Unity Connection can perform a file integrity check as part of the restore operation. This is advisable to ensure that the files are valid and have not been corrupted during the backup or restore operations.

g) Select **Restore** to begin the restore of the selected .tar file to the server.

As with the restore operation, you can view the restore operation log file for each restored component.

Also as with a restore operation, the time it takes to restore depends on the size of the database and the components restored.

Step 5 Restart the new Unity Connection server. In case of a cluster server, reboot the publisher server.

Step 6 (Cluster only) Once the publisher reboots, run the following command on Command Line Interface (CLI) on the subscriber server to copy the data from the publisher to the subscriber server:

```
utils cuc cluster overwritedb
```

Step 7 (Cluster only) Run the following CLI command on either the publisher or subscriber server to check the status of the Unity Connection cluster:

```
show cuc cluster status
```

Verify that the status of publisher server is Primary and subscriber server is Secondary. Test and validate it before moving it back into production.

Note
(Applicable to 14 SU4 or later) If you are using SpeechView with Cisco Webex in-house transcription service, onboard the Subscriber Server of the Unity Connection Cluster on Cisco Webex Cloud-Connected UC. For more details on

Onboarding Unity Connection server on Cisco Webex Cloud-Connected UC, refer https://help.webex.com/en-us/article/nzt6c0b/Set-up-Webex-Cloud-Connected-UC-for-on-premises-devices.

Viewing the Restore Status

To Check the Restore Status in Disaster Recovery System

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Restore > Current Status**. The Restore Status window displays.

The Status column in the **Restore Status** window shows the percentage of restore process completed.

Step 3 To view the restore log file, select the log filename link.

Viewing the Restore History

To View the Restore History in Disaster Recovery System

Procedure

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Restore > History**. The Restore History window displays.

Step 3 On the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

Note
The **Restore History** window displays only the last 20 restore jobs.

About System Restore Tool

The System Restore Tool is a new tool introduced in Unity Connection that allows the administrator to take either manual backup or schedule backup at specified intervals of time. The tool creates restore points that the administrator can use to restore data. For example, if the database is corrupted, the data can be restored using restore points.

Types of System Restore Points

The administrator can create following types of restore points using System Restore Tool:

- **Recent**: Allows you to restore the data from the most recent backup stored on the server.
- **Daybefore**: Allows you to restore the data from the backup before the recent data backup stored on the server.
- **Temp**: Allows you to restore data from the manual backup created at a particular instance of time. The administrator can create the Temp restore point through the run cuc sysrestore backup_temp CLI command only. For more information on the CLI command, see the "run cuc sysrestore backup_temp section" of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/12_0_1/CUCM_BK_CA8D6400_00_cucm-cli-reference-guide-120_chapter_001.html

Note Whenever the data backup is initiated, the data from Recent restore point is copied to Daybefore and current restore point is marked as Recent. This cycle continues with each scheduled backup, which helps in maintaining the integrity of the backup and consuming less space (less than 2GB) to store the restore points efficiently.

Creating a Restore Point task

Do the following tasks to create restore points using System Restore Tool.

1. Create a user with mailbox with an alias "system-backup-and-restore-admin" and assign him a corporate email id to receive the restore point creation alerts or failure notifications. For more information on how to create a user, see Users chapter of *System Administration Guide for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Note Skip this task, if such user already exists.

2. If you want to schedule automatic backup, enable the Create Backup Restore Point task to automate backup. See Enabling Create Backup Restore Point
3. If you want to create manual backup, run the run cuc sysrestore backup_tem CLI command.

Note In case of Unity Connection cluster, take backup of publisher and subscriber server separately.

Enabling Create Backup Restore Point

Do the following steps to enable the Create Backup Restore Point task for automatic backup.

Procedure

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Navigate to **Tools > Task Management** and select **Create Backup Restore Point**.

Step 3 Go to **Edit** and select **Task Schedules**.

Step 4 On the Task Schedules page, enter the required information to schedule the task.

Step 5 Click **Save** to apply the settings.

Restoring Data using Restore Points task

The administrator can restore data using restore points created through System Restore Tool.

Note During restore operation, the tool specifies the timestamp of the restore point, the count of the messages against the user aliases, and also lists the users which will be lost after restore operation. The user aliases that are reported to be lost after restore are the aliases created after the restore point creation.

To restore the data using restore points, run the following CLI command:

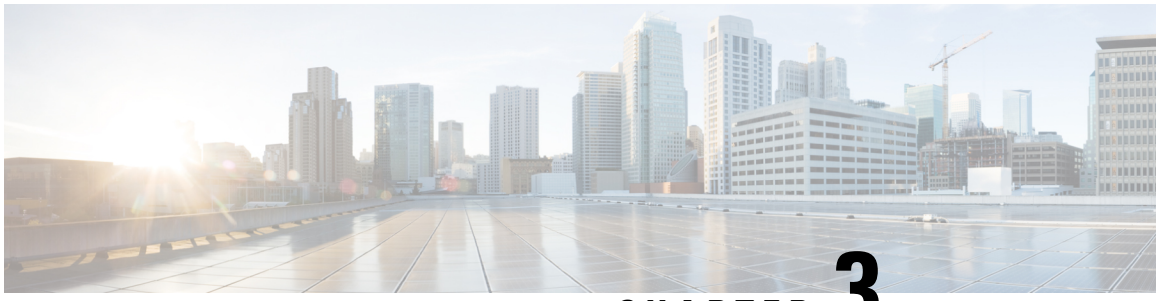
```
run cuc sysrestore restore_operation <restore mode> <restore point>
```

where,

- restore mode can be database, config, or both
- restore point can be Recent, Daybefore or Temp

Restore mode specifies the data that you want to restore. For example, if you specify database as restore mode, only database is restored.

Note If you specify config or both as restore mode, you need to restart the server to restore the data successfully.



CHAPTER 3

Upgrading Cisco Unity Connection

- Introduction, on page 43
- Upgrade Types, on page 43
- Status of Unity Connection Cluster During an Upgrade and Switch version, on page 47
- Duration of Upgrade, on page 48
- Prerequisites for Upgrade, on page 48
- Upgrade Considerations with FIPS Mode, on page 51
- Task list to Upgrade to Unity Connection Shipping Version 14, on page 51
- Upgrading the Unity Connection Server, on page 55
- Switching to the Upgraded Version of Unity Connection Software, on page 57
- Applying COP file from a Network Location, on page 58
- Rollback of Unity Connection, on page 59

Introduction

You need to upgrade from the current version of Cisco Unity Connection to a higher version to use the new features supported with the new version. When you upgrade a server, the new version of Unity Connection is installed in a separate disk partition known as inactive partition. To activate the new version, you need to perform switch version. The following are the two ways to switch to the new version:

- Automatic Switching: Allows you to automatically switch to the new version of Unity Connection as part of the upgrade process.
- Manual Switching: Allows you to manually switch to the new version of Unity Connection after the successful completion of upgrade.

If you need to revert the server to the previous version, you can rollback to the previous version.

Upgrade Types

The Unity Connection upgrade files are available as ISO images or COP (Cisco Option Package) files. You can use either of the following interfaces to upgrade Unity Connection:

- Command Line Interface (CLI)
- Cisco Unified OS Administration web interface.

You must save the COP files on a Network Location FTP/SFTP server accessible during upgrade. ISO image can be saved on a local DVD or on a network location. The performance of the upgrades can be monitored through CLI or Cisco Unified Operating System Administration interfaces.

Table 1 explains the upgrade types and supported upgrade paths from one version to another.

Table 5: Upgrade Matrix for Cisco Unity Connection

Upgrade Type	Upgrade Path	Description
Service Update (SU)	Examples of supported paths: • 12.x.x/12.x.xSUx1 to 12.x.xSUx2 • 11.x.x/11.x.xSUx1 to 11.x.xSUx2	• SU is installed on the inactive partition to which you later on. • ISO images are non-bootable images not meant for i

Upgrade Type	Upgrade Path	Description
Refresh Upgrade (RU)	Examples of supported paths: • 10.5.2SU10 or earlier to 14 • 11.5.1SU9 or earlier to 14 **Note** • For 10.5(1) to 14, you must follow an intermediate upgrade path. Example: 10.5(1) to 11.x or later and then 11.x or later to 14. • Starting with 14SU2 release, upgrades from release 10.5.2 are blocked so a direct upgrade attempt will fail as an usupported upgrade.	• If the operating system version of the Unity Con during an upgrade, it is referred to as a Refresh U • You need the following COP files in same sequen below before performing this upgrade: • ciscocm.enable-sha512sum-2021-signing-k • ciscocm.cuc_upgrade_12_0_v1.3.cop.sgn • Select option "Reboot to upgraded partition" on to new version if the upgrade is successful" as "Y proceed with the upgrade. **Note** Options "Do not reboot after upgrade" on GUI a new version if the upgrade is successful" set as " not supported.If these options are selected, the sy reboot and pick the upgraded version.
	Examples of supported paths: • 11.5.1SU10 or later to 14	• You need the following COP file before performi • ciscocm.cuc_upgrade_12_0_v1.3.cop.sgn • Select option "Reboot to upgraded partition "Switch to new version if the upgrade is succ on CLI and proceed with the upgrade. **Note** Options "Do not reboot after upgrade" on G to new version if the upgrade is successful" CLI are not supported.If these options are s system will still reboot and pick the upgrad
	12.0.1SU4 or earlier to 14	• You need the following COP file before performi • ciscocm.enable-sha512sum-2021-signing-k • Select option "Reboot to upgraded partition "Switch to new version if the upgrade is succ on CLI and proceed with the upgrade. **Note** Options "Do not reboot after upgrade" on G to new version if the upgrade is successful" CLI are not supported.If these options are s system will still reboot and pick the upgrad
	12.0.1SU5 or later to 14	

Upgrade Type	Upgrade Path	Description
		• No COP file is required for this upgrade path. • Select option "Reboot to upgraded partition" on GUI to new version if the upgrade is successful" as "Yes" proceed with the upgrade. **Note** Options "Do not reboot after upgrade" on GUI and " new version if the upgrade is successful" set as "No" not supported.If these options are selected, the syste reboot and pick the upgraded version.
Level 2 (L2)	12.5.1SU3 or earlier to 14	• If the operating system version of the Unity Connect change during an upgrade, it is referred to as an Lev upgrade. • You need the following COP file before performing t • ciscocm.enable-sha512sum-2021-signing-key-v • The new version is installed on the inactive partition t can switch later on.
	12.5.1SU4 or later to 14	• No COP file is required for this upgrade path.
COP file, for more information, see the Applying COP file from a Network Location	Fix for the same version	• COP files are installed on the active partition and yo uninstall them. Contact Cisco TAC to uninstall COP

Note If you are upgrading Unity Connection to 14 and later, then after completion of successful upgrade, you must reinstall the set of available locales that are compatible with the upgraded version. To install locale, refer https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg/b_14cuciumg_chapter_0100.html.

Before installing locales, you must stop the Connection Conversation Manager and Connection Mixer services through Cisco Unity Connection Serviceability page. It is recommended that you should install the locales on Unity Connection through Command Line Interface.

For more information on CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

To complete the locale update, restart the Cisco Tomcat service across the entire cluster (both publisher and subscriber nodes). This ensures that the Cisco Unity Connection GUI is synchronized and that the correct language settings are displayed on both the publisher and subscriber nodes.

Caution After successful upgrade to Unity Connection 14, if you need to revert the server to previous software version, you can switch version the software to older version. After that, you can not upgrade the server to any pre 14 release (for example: 11.5(1) or 12.0(1)). In addition to this, If the upgrade from any previous releases to Unity Connection 14 fails for any reason, then also you cannot upgrade the server to pre 14 release. To troubleshoot the issue, contact Cisco TAC.

If administrator wants to upgrade the server to pre 14 release in above scenarios, fresh cluster rebuild is required by performing DRS backup and restore before upgrade.

If you are upgrading Unity Connection from 11.5(1) or 12.0(1) as base release to 14 and later, then you must rename custom role "Read Only Administrator" to different name on base release before upgrade.

Note The procedure for upgrading Unity Connection to any Service Update (SU), is similar to RU and L2 upgrade.

Status of Unity Connection Cluster During an Upgrade and Switch version

When a Unity Connection cluster is upgraded, the publisher server is completely disabled for the entire duration of upgrade but the subscriber server continues to provide services to users and callers. However, the performance of the cluster is affected in the following ways:

- During a switch version of the publisher server, the phone system routes calls to the subscriber server. Outside callers and Unity Connection users can leave voice messages during this time. However, these messages are processed differently and do not appear in the publisher server's web inbox after the subscriber server completes its switch version.
- Unity Connection users can use the telephone user interface (TUI) to play messages recorded or saved before the switch version starts but cannot play the messages recorded or saved during the switch version.
- Unity Connection may not retain the status of messages. For example, if a user plays a message during the switch version, the message may be marked as 'New' again after the switch version. Likewise, if a user deletes a message during the switch version, the message may reappear after the switch version.
- User can access Unity Connection using clients such as, ViewMail for Outlook, Web Inbox and Jabber during upgrade. However, during switch version, user cannot access these clients. In case of RU, these clients are not accessible during complete upgrade..
- Administrator users can make configuration changes using any of the administration applications, such as Cisco Unity Connection Administration and Cisco Unified Operating System Administration during upgrade. However, Unity Connection does not allow provisioning and configuration changes through administration applications or VMREST during the switch version. In case of RU, provisioning and configuration are not allowed in complete upgrade duration.
- Intrasite, intersite or HTTPS networking with other servers is disabled for the duration of the switch version. Directory changes made on the other servers in the network are not replicated to the server or cluster until the switch version is complete.

Note The Automatic Switch version option is not available on clusters which contain Unity Connection and Cisco Unified Contact Center Express nodes. For clusters with Cisco Unity Connection and Cisco Unified Contact Center Express, 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

Duration of Upgrade

Under ideal network conditions, an upgrade process takes approximately two hours to complete on each server. Therefore, a Unity Connection cluster takes four hours to upgrade to a higher version. Depending on the data size of the server, the switch version process might take some more time.

If you are upgrading in a slow network condition, the upgrade process may take longer time than expected. It is always recommended to upgrade Unity Connection during off-peak hours or during a maintenance window to avoid service interruptions.

Tip You can reduce the duration of upgrade process by asking users to permanently delete items in the deleted items folder before starting the upgrade. This saves time as deleted items are not copied.

Prerequisites for Upgrade

Before beginning the upgrade process, you must consider the following points for a successful upgrade:

- Ensure that you have a good network connection to avoid service interruptions during upgrade.
- You must have a Secure File Transfer Protocol (SFTP) or File Transfer Protocol (FTP) server in place when upgrading from a network location.
- Check the current version and determine the version to which you want to upgrade. See the release notes of the new version for more information. Release notes are available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.

Note If the *LowSwapPartitionAvailableDiskSpace* RTMT alert appears on a Cisco Unity Connection Release 14 server, consider the following recommendations:

- Upgrade to Release 15, where this issue has been resolved. If upgrade is not possible, rebuild the cluster on Release 14 with a larger OVA to increase available swap space.

- Determine if you need COP files depending on the upgrade process. Download the COP and ISO image files from: http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm
- Backup all the existing data. For more information on backup and restore, see the Backing Up and Restoring Cisco Unity Connection Components chapter.

- Update the following virtual machine settings on both publisher and subscriber server through VMware vSphere client.

Note For more information on changing the Guest Operating System and network adapter, see the corresponding Readme of the OVA template at https://software.cisco.com/download/home/283062758/type.

- Confirm that the status of both publisher and subscriber servers is active and they can answer calls. Follow the given steps to confirm the server status in a cluster:

  Sign in to Cisco Unity Connection Serviceability.

  Expand Tools and select Cluster Management.

  Check the server status in a cluster.

  In addition to this, confirm the running state of database replication using the CLI command show cuc cluster status.

Note After confirming the status of publisher server as Primary and subscriber server as Secondary, start the upgrade process first on publisher server and then on subscriber server.

- Before upgrading to Unity Connection Release 15, rename the notification templates if created with the below mentioned names.

  Default_Missed_Call

  Default_Missed_Call_With_Summary

  Default_Scheduled_Summary

  Default_Voice_Message_With_Summary

  Default_Dynamic_Icons

  Default_Actionable_Links_Only

  If not renamed the mentioned notification templates gets replaced with default notification templates of release 15.

- Before upgrading to Unity Connection Release 15, make sure the display name of default notification devices is not changed for any of the user. If changed then update notification devices to the default name.

  To check the users whose default notification device name is changed, execute below query:

```
run cuc dbquery unitydirdb SELECT COUNT(*) AS num_sys_notdevices, USR.alias,
ND.subscriberobjectid FROM tbl_notificationdevice AS ND INNER JOIN vw_user USR ON
ND.subscriberobjectid = USR.objectid WHERE ((ND.devicename IN ('Home Phone', 'Work
Phone', 'Mobile Phone', 'Pager', 'SMTP') AND ND.displayname = ND.devicename) OR
(ND.devicename='HTML' AND ND.displayname IN ('HTML', 'HTML Missed Call', 'HTML Scheduled
 Summary'))) GROUP BY ND.subscriberobjectid, USR.alias HAVING COUNT(*) != 8
```

- Initiate a pre upgrade test before starting the upgrade process using the CLI command

run cuc preupgrade test

- If you have legacy and PLM based licenses in earlier releases, you must migrate the licenses to Cisco Smart Software Licensing before upgrade to Unity Connection Release 15. For more information on Cisco Smart Software Licensing flow in Unity Connection see Managing Licenses chapter of *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 15*.

Caution For successful upgrade of Unity Connection from 12.0(1) to any higher releases, make sure the system does not exist in Enforcement mode before upgrade.For more information on Enforcement mode, see Enforcement Policy on Unity Connection section.

- Unity Connection Release 15 supports ESXi version of 7.0 U3. For more information on Virtual Hardware settings, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html.
- The Exchange 2003, 2007, 2010, 2013 is end of support now. Therefore, it is recommended to delete the Unified Messaging Service configured with Exchange 2003 or 2007 or 2010 or 2013 while upgrading to Unity Connection Release 15 or later. Now, create a new Unified Messaging Service with supported Exchange version 2016 or 2019 to avoid any issues while using Unified Messaging Services.

Note In the upgrade logs, it is observed that there is time discrepancy or time jumps during certain intervals. This time jump is an expected behavior since the hardware clock is disabled until the system synchronizes with the NTP server.

Caution The **CUC Export Restricted Authorization Key (CUC-SL-EXRTKY-K9=) license is now End-of-Sale (EOS)**.

End-of-Sale Date: August 2, 2020.

End-of-Support Date: August 31, 2025.

This license is no longer available for new purchases. For more information, refer https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-licensing/eos-eol-notice-c51-744285.html

If encryption is required for export-restricted virtual accounts:

1. Customers with existing licenses can continue using them until the End-of-Support date.

2. For new installations or upgrades to Cisco Unity Connection 14 or later, this license is no longer supported.

3. The recommended replacement for this license is: **Export Restricted Authorization Key for CUCM-Smart Licensing (CUCM-SL-EXRTKY-K9=)**

4. Contact your Cisco representative or reseller to explore alternative licensing options.

Upgrade Considerations with FIPS Mode

If you are performing upgrade with FIPS enabled Unity Connection Release to 14 and later, you must consider the below limitations for a successful upgrade:

- Before upgrading Unity Connection using FIPS-enabled mode, make sure that the security password length is greater than or equal to 14 characters to meet FIPS compliance.
- In Unity Connection Release 14, the IPsec policies with DH group key values 1, 2 or 5 are disabled. If you are upgrading Unity Connection to Release 14 with FIPS enabled and IPse configured, then you must perform any one of the given procedure for successful upgrade to Unity Connection 14
  - Delete the previously configured IPsec policies and perform the upgrade. After the upgrade is complete, reconfigure the IPsec policies with DH groups 14–18.
  - Install the **ciscocm_ipsec_groupenhancement_fips_<version>.cop** COP file that supports DH groups 14–18, reconfigure the IPsec policies and then perform an upgrade.

Note If you disable the FIPS mode after installing the COP file, the IPsec configuration page does not appear.

- If you are upgrading Unity Connection which has IPsec configured using a certificate-based authentication with self-signed certificate, then you must reconfigure the IPsec policy with a CA-signed certificate foe a successful upgrade.
- In FIPS mode, if you have configured Unified Messaging with NTLM web authentication mode then you must select a Basic authentication mode before upgrading Unity Connection to 14 and later. NTLM web authentication mode is no longer supported.
- If you are upgrading from any release of Unity Connection 12.5 in FIPS mode to Unity Connection 14SU2 and later, make sure to install COP File **ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512** on both nodes of cluster before upgrade.

For more information on FIPS mode, see "FIPS Compliance in Cisco Unity Connection" chapter of *Security Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

Task list to Upgrade to Unity Connection Shipping Version 14

Do the following tasks to upgrade an Unity Connection server:

1. If you are running the current version of Unity Connection on a physical server then you must replace it with a virtual server. See the Migrating a Physical Server to a Virtual Machine.

   If you are already running the current version on a virtual server, make sure it is compatible with the upgraded version. See the Cisco Unity Connection 14 Supported Platform List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.html.

Note If you are performing an L2 upgrade, make sure that the Platform SOAP services are running on both the Unity Connection servers to successfully upgrade using Prime Collaboration Deployment. SOAP services can be enabled on both the servers using Cisco Unified Serviceability page. For more information on PCD, see 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.

2. If you are upgrading during non business hours, run the following command on the standalone server or the publisher server to speed up the upgrade process:

   utils iothrottle disable

   If you are upgrading during a maintenance window, you can speed up the upgrade by disabling the throttling. This decreases the time required to complete the upgrade but affects Unity Connection performance.

Caution You cannot disable throttling during the upgrade process. If you want to disable the throttling process, you must first stop upgrade, disable throttle, and restart the Unity Connection server. Once the server is active again, begin the upgrade process.

3. Migrate all the licenses (legacy and PLM based) before you upgrade to Unity Connection 14 server. For more information, see the Migrating Licenses section.
4. Confirm if you require COP file for the upgrade process and download file from https://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm
5. Apply the COP file using the steps listed in the Applying COP file from a Network Location.
6. Follow the upgrade process on the standalone server:
   - (RU upgrades only) Upgrade the server by performing the steps mentioned in the Upgrading the Unity Connection section. The server automatically switches to the new version after completing the upgrade.
   - (L2 upgrades only) Upgrade the server using the steps mentioned in the Upgrading the Unity Connection section. Switch to the upgraded software to complete the upgrade process following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software section.
7. Follow the upgrade process on the Unity Connection cluster:
   - (RU upgrades only) Upgrade the publisher server following the steps mentioned in the Upgrading the Unity Connection Server section. The server automatically switches to the new version after completing the upgrade.

     Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server section. The server automatically switches to the new version after completing the upgrade.
   - (L2 upgrades only) Upgrade the publisher server using the steps mentioned in the Upgrading the Unity Connection Server section.

Caution In case of L2 upgrade of a cluster, do not restart or perform switch version on the publisher server before completing the upgrade on subscriber server otherwise cluster does not function properly.

Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server section.

Switch to the upgraded software first on the publisher server and then on the subscriber server following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software section.

8. Confirm that publisher server has Primary status and subscriber server has Secondary status.

9. After successful upgrade to Unity Connection 14, the product remains in Evaluation Mode until you register the product with CSSM or satellite.

10. If you are performing an upgrade from a FIPS enabled Unity Connection Release to Unity Connection 14, make sure to follow the steps for regenerating certificates before using any pre-existing telephony integrations. To learn how to regenerate certificates, see the Regenerating Certificates for FIPS section of the "FIPS Compliance in Cisco Unity Connection" chapter in *Security Guide for Cisco Unity Connection Release 14,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

11. If Secure SIP call is configured on the system using SIP Integration then after successful upgrade, generate and upload RSA based Tomcat certificates. To learn how to regenerate certificates, see Settings for RSA Key Based certificates section of the "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter in *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.

Note Verify that the value entered in **X.509 Subject Name** field on SIP Trunk Security Profile Configuration page of Cisco Unified Communication Manager is the FQDN of the Unity Connection server

12. Cisco Unity Connection supports HAProxy which frontends all the incoming web traffic into Unity Connection offloading Tomcat. HAProxy sends the request internally to Tomcat via HTTP. For information on new ports which should be opened after successful upgrade, see chapter IP Communications Required by Cisco Unity Connection in *Security Guide for Cisco Unity Connection Release 14,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

13. If Next Generation Security over HTTPS interface is configured on the system then after successful upgrade to Unity Connection 14, the configured settings of HTTPS ciphers get reset. You must reconfigure the HTTPS ciphers on Enterprise Parameter page of Cisco Unity Connection Administration and restart the Tomcat service.

Note In case of a cluster, you must configure the HTTPS ciphers on publisher server and restart the Tomcat service on each node to reflect the changes.

14. If Specific License Reservation(SLR) mode is enabled on the system, then after successful upgrade to Unity Connection Release 14, you must return all reserved licenses to Cisco Smart Software Manager(CSSM) and reconfigure SLR with new version licenses. For more information on configuration of Specific License Reservation in Unity Connection, see the Configuring Specific License Reservation in Unity Connection section of the "Managing Licenses" chapter in *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

15. Cisco Unity Connection supports SAML-based Single Logout (SLO). The SLO allows you to log out simultaneously from all sessions of a browser that you have signed in using Single Sign-on (SSO). SLO does not close all the running sessions at the same time. If SAML SSO mode is enabled with Microsoft ADFS 2.0 configuration on the system, then after successful upgrade to Unity Connection Release 14 you must follow steps mentioned in section SAML-Based Single Logout (SLO) of *Quick Start Guide for SAML SSO Access* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/quick_start/guide/b_14cucqssamlsso.html.

16. To avoid upgrade related issues it is recommended to run Pre Upgrade COP file before upgrade. The COP file will run a series of tests to check the pre-upgrade health and connectivity of your system. If the COP file highlights issues that need to be addressed, fix them before proceeding with the upgrade. After sucessful upgrade it is recommended to run Post Upgrade COP file to verify the configuration of system. Download the COP files from http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm.

Caution *(Applicable to 12.5SU1, 12.5SU2, 12.5SU3 releases only)* For upgrading Unity Connection to release 14, Pre and Post Upgrade COP files should be installed via CLI only.

17. *(Applicable only to Cisco Unity Connection 14SU2 Release)* If you are creating a new Intrasite link or if there is any existing Intrasite link between two nodes of Unity Connection in FIPS mode with one node on 14SU2 release and other node on any release lower than 14SU2, then only message delivery between two nodes will work. Object(users, system distribution lists if applicable, partitions, search spaces and Unity Connection locations) synchronization is not supported. For object synchronization to work, you must upgrade all the Unity Connection nodes in network to 14SU2 release.

18. After successful upgrade to Unity Connection 14SU2, if you need to perform rollback of server from 14SU2 to any older release then you must re-register the product with CSSM or satellite using a registration token for successful functioning of Smart Licensing as applicable to the release.

19. If Secure SMTP is enabled on the system, then after successful upgrade to Unity Connection Release 14SU2 you must reconfigure the Secure SMTP feature using Cisco Unity Connection Administration. For more information, see Configure SMTP Client Communication section of the chapter "Messaging" of the System Administration Guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

20. CUNI Subscriptions will be removed from Cisco Unity Connection server database, if you perform a refresh upgrade to Unity Connection 14. Make sure to perform re-subscription after successful upgrade of the cluster.

21. If you are performing upgrade to Unity Connection 14 SU3 and later releases from any of the older release, make sure to reconfigure permissions on Azure Portal after sucessful upgrade. To learn how to reconfigure the permissions, see Step 4g of the section "Task List for Configuring Unified Messaging with Office 365" of the chapter "Configuring Unified Messaging" of the *Unified Messaging Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/unified_messaging/guide/b_14cucumgx.html.

22. SpeechView with Cisco Webex in-house transcription service is the only available option after upgrade to 14 SU4 or later in order to use SpeechView feature.

Note To use SpeechView with Cisco Webex in-house transcription service after upgrade to 14 SU4, refer "SpeechView Cisco Webex in-house transcription service" chapter available at *System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html

23. In order to use SpeechView feature with Cisco Webex in-house transcription service in Digital Networking, make sure to upgrade all nodes in the network to release 14 SU4 or later.
24. If Unity Connection Cluster has been onboarded on Cisco Webex Cloud-Connected UC before upgrade to 14 SU4, then after the upgrade, Telemetry module may take up to 75 minutes to update its status online on Cisco Webex Cloud-Connected UC. To check the Telemetry module status, refer View the node status for Telemetry Module Inventory.
25. After the upgrade of Unity Connection Cluster to release 14 SU4 or later , if you are using SpeechView feature, restart the "**Connection SpeechView Processor**" service on the Connection Serviceability page of the Pubisher sever of the Unity Connection Cluster once the Telemetry module status is online on Cisco Webex Cloud-Connected UC.

Upgrading the Unity Connection Server

Do the following steps to upgrade a standalone server or a cluster. In case of a cluster, follow the steps first on the publisher server and then on the subscriber server.

Procedure

Step 1 Do any one of the following:

- Copy the ISO file to a folder on an FTP or SFTP server that the Unity Connection server can access.
- Insert the DVD with the ISO file of the Unity Connection server that you want install into the disk drive of the server.

Step 2 Sign in to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, select **Install/Upgrade**.

Step 4 *(Applicable only for subscriber server) (Optional)* On the Software Installation/Upgrade page, check the **Use download credentials from Publisher** check box to use the source configuration provided for the publisher server and move to Step 13.

Step 5 In the **Source** field, select any one of the following:

- **Remote Filesystem**: Select this option to upgrade from remoter server and follow this procedure.
- **DVD/CD**: Select this option to upgrade from disk drive and move to Step 11.
- **Local Filesystem**: Select this option to use the previously downloaded ISO or COP files for the upgrade.

Step 6 In the **Directory** field, enter the path of the folder that contains the upgrade file.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the upgrade file is in the upgrade folder, you must enter /upgrade).

If the upgrade file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

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

Step 8 In the **User Name** field, enter the alias that is used to sign in to the remote server.

Step 9 In the **User Password** field, enter the password that is used to sign in to the remote server.

Step 10 In the **Transfer Protocol** field, select the applicable transfer protocol.

Step 11 In the **SMTP Server** field, enter the IP address of the SMTP server.

Step 12 In the **Email Destination** field, enter your email address along with the SMTP server.

Step 13 Select **Next**.

Step 14 Select the upgrade version that you want to install and select **Next**.

The upgrade file is copied to the hard disk of the Unity Connection server. When the file is copied, a screen displaying the checksum value appears.

Step 15 Verify the checksum.

Step 16 On the next page, monitor the progress of the upgrade.

Caution
If you loose your connection with the remote server or close your browser during this step, you may see the following warning when you try to view the Software Installation/Upgrade page again:

Warning: Another session is installing software, click Assume Control to take over the installation. To continue monitoring the upgrade, select Assume Control.

To continue monitoring the upgrade, select Assume Control.

Step 17 Select **Next**.

During the initial phase of upgrade, the Installation Log text box in Cisco Unified Operating System Administration is updated with the information on the progress of the upgrade. To confirm the completion of upgrade, open the console of the Unity Connection server and make sure that a message indicating the completion of upgrade appears on the screen along with the login prompt.

Step 18 Select **Finish**.

Step 19 To verify if the upgrade is successful, run the following CLI commands:

- show cuc version: Displays the version of Unity Connection server in both active and inactive partitions. The upgraded Unity Connection version is in the inactive partition and old version is in the active partition.
- utils system upgrade status: Displays the status of the upgrade that you performed. This command should display the message for successful upgrade along with the upgraded version.

Switching to the Upgraded Version of Unity Connection Software

After completing the upgrade process, you can select either manual switch version or automatic switch version. The method that you choose depends on the type of upgrade that you are doing. During the upgrade process, the wizard prompts you to choose whether to switch the software version automatically by rebooting to the upgraded partition, or whether to switch the version manually at a later time.

Automatic Switching

The table below lists the automatic switching method to use for each type of upgrade.

Upgrade Type	When prompted, choose...	Result
L2 Upgrade	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	When you choose this option, the system reboots to the new software version.
Refresh Upgrade	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	Choose this option to use the new upgraded software version immediately following the upgrade. **Note** Option "Do not reboot after upgrade" is not supported on GUI and if selected, the system will still reboot and pick the upgraded version.

You can perform the switch version running the CLI command utils system switch-version. The system automatically reboots after the switch version.

Manual Switching

If you select not to automatically switch to the upgraded partition at the end of the upgrade, do the following procedure when you are ready to switch partitions.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the **Settings** menu, select **Version**.

Step 3 On the Version Settings page, select **Switch Versions**, to start the following activities:

- Unity Connection services are stopped.
- Data from the active partition is copied to the inactive partition. Note that the messages are stored in a common partition, therefore they are not copied.
- The Unity Connection server restarts and switches to the newer version.

Applying COP file from a Network Location

Procedure

Step 1 Copy the Cisco Option Package (.cop) file on an FTP or SFTP server that the server can access.

Step 2 Sign in to Cisco Unified Operating System Administration.

If you are upgrading the subscriber server in a Unity Connection cluster, type the following address to access Cisco Unified Operating System Administration:

http://<Unity Connection_servername>/cmplatform

Step 3 From the Software Upgrades menu, select Install/Upgrade.

Step 4 On the Software Installation/Upgrade page, in the Source field, select Remote Filesystem.

Step 5 In the Directory field, enter the path to the folder that contains the .cop file.

If the .cop file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the .cop file is in the cop folder, you must enter /cop).

If the .cop file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

Step 6 In the Server field, enter the server name or IP address.

Step 7 In the User Name field, enter the alias that is used to sign in to the remote server.

Step 8 In the User Password field, enter the password that is used to sign in to the remote server

Step 9 In the Transfer Protocol field, select the applicable transfer protocol and select Next.

Step 10 Select the software that you want to install, and select Next.

The .cop file is copied to the virtual hard disk on Unity Connection server. When the file is copied, a screen displays the checksum value.

Step 11 Verify the checksum and select Next to begin the installation.

During the upgrade, the value of the Status field is Running. When the upgrade process is complete, the value of the Status field changes to Complete.

Note
- All command-line interface sessions are terminated automatically.
- The Cisco Tomcat Service can take several minutes to restart automatically.

Step 12 Sign out from the Cisco Unified Operating System Administration application.

Step 13 Run the CLI command utils service list to confirm that the Cisco Tomcat service is in the Running state.

Rollback of Unity Connection

After upgrading the Unity Connection version, you can rollback to the software version that was running before the upgrade by switching to the software version on inactive partition.

Caution If you revert to the version on the inactive partition in case of RU upgrade rollback from 14 to 12.x or 11.x or 10.x versions, you cannot later switch to the newest version again. Instead, you must reinstall the upgrade as documented in this guide.

Important Considerations for Rollback

1. Do not make any configuration changes during the rollback because the changes are lost after the rollback.
2. In an cluster setup, do not switch versions on both the first and second servers at the same time. Perform switch version on the second server only after you have switched versions on the first server.
3. Users and mailbox stores that were added after the upgrade, no longer exist after you rollback to the version on inactive partition. The new users and mailbox stores are deleted.
4. All messages are preserved for Level 2 Upgrade Rollback, but for the users that were added after upgrade, their messages are orphaned as the users no longer exist after rollback. These messages are moved to the undeliverable messages folder. However the messages for Refresh Upgrade Rollback are not preserved for existing users or any new users added after upgrade
5. If you moved mailboxes from one mailbox store to another after upgrading, those mailboxes are moved back to the mailbox stores they were in before the upgrade.
6. A future delivery folder is created for users to mark messages for future delivery. If you revert to a version that supports future delivery but the future delivery folder has not been created for the user as yet, the messages in the future delivery folder for the new version are moved to the undeliverable messages folder.
7. (Unity Connection 8.5 and earlier only) If a user rollbacks to Unity Connection version 8.5 or earlier from a current version that is 8.6 and higher, then following limitations are faced:
   - No voice messages are left after the rollback.
   - No administrator settings are preserved after the rollback.
8. No administrator settings are preserved after the rollback.
   a. Revert to the Guest Operating System version as earlier (before upgrade).
   b. Modify the network adapter to the adapter type as earlier (if you changed after upgrade).

Rollback Scenarios

You can revert a single Unity Connection server or a cluster to the version on inactive partition.

To rollback a Unity Connection cluster, you should rollback both the servers, first the publisher and then the subscriber. After the successful rollback of both the publisher and subscriber servers, reset the replication between the two servers running the following CLI commands:

Stop the replication on subscriber server with the CLI command utils dbreplication stop.

Stop the replication on publisher server with the CLI command utils dbreplication stop.

Reset the replication running the CLI command utils dbreplication reset all on the publisher server.

After the reset of replication between the two servers, check the cluster status running the CLI command show cuc cluster status utils system restart on both publisher and subscriber.

Rollback a Unity Connection Server to the Version in the Inactive Partition

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, select Version and the Version Settings window displays.

Step 3 Select the Switch Versions option. After you confirm that you want to restart the system, the system restarts that might take up to 15 minutes.

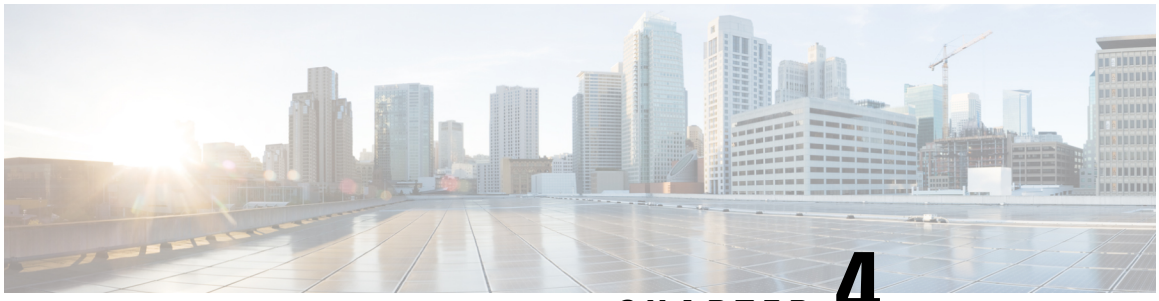
Step 4 Follow the given steps to confirm that the switch version is successful:

a. Sign in to Cisco Unified Operating System Administration.

b. In the Settings menu, select Version. The Version Settings window displays the product version.

c. Confirm that the active partition runs the correct version of Unity Connection server and all critical services are in the Running state.

d. Sign in to Cisco Unity Connection Administration and confirm that the configuration data exists.



CHAPTER 4

Configuring Cisco Unity Connection Cluster

- Introduction, on page 61
- Task List for Configuring a Unity Connection Cluster, on page 61
- Administering a Unity Connection Cluster, on page 62
- How a Unity Connection Cluster Works, on page 72
- Effects of Split Brain Condition in a Unity Connection Cluster, on page 73

Introduction

The Cisco Unity Connection cluster deployment provides high availability voice messaging through the two servers that run the same versions of Unity Connection. The first server in the cluster is the publisher server and the second server is the subscriber server.

Task List for Configuring a Unity Connection Cluster

Do the following tasks to create a Unity Connection cluster:

1. Gather Unity Connection cluster requirements. For more information, see *System Requirements for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html .
2. Install the publisher server. For more information, see the Installing the Publisher Server section.
3. Install the subscriber server. For more information, see the Installing the Subscriber Server section.
4. Configure the Cisco Unified Real-Time Monitoring Tool for both publisher and subscriber servers to send notifications for the following Unity Connection alerts:
    - AutoFailbackFailed
    - AutoFailbackSucceeded
    - AutoFailoverFailed
    - AutoFailoverSucceeded
    - NoConnectionToPeer
    - SbrFailed

For instructions on setting up alert notification for Unity Connection alerts, see the "Cisco Unified Real-Time Monitoring Tool" section of the Cisco Unified Real-Time Monitoring Tool Administration Guide for the required release, available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

5. *(Optional)* Do the following tasks to customize the cluster settings on the publisher server:

   Sign in to Cisco Unity Connection Administration.

   Expand **System Settings > Advanced and** select **Cluster Configuration**.

   On the Cluster Configuration page, change the server status and select Save. For more information on changing the server status in a cluster, see Help> This Page.

Administering a Unity Connection Cluster

You must check the Unity Connection cluster status to ensure that the cluster is correctly configured and working properly. It is also important to understand the different server status in a cluster and the effects of changing a server status in a cluster.

Checking the Cluster Status

You can check the Unity Connection cluster status either using web interface or Command Line Interface (CLI).

Steps to Check the Unity Connection Cluster Status from Web Interface

Procedure

Step 1 Sign in to Cisco Unity Connection Serviceability of either publisher or subscriber server.

Step 2 Expand Tools and select Cluster Management.

Step 3 On the Cluster Management page, check the server status. For more information about server status, see the Server Status and Its Functions in Unity Connection Cluster section.

Steps to Check Unity Connection Cluster Status from Command Line Interface (CLI)

Procedure

Step 1 You can run the show cuc cluster status CLI command on the publisher server or subscriber server to check the cluster status.

Step 2 For more information about server status and its related functions, see the Server Status and Its Functions in Unity Connection Cluster section.

Managing Messaging Ports in a Cluster

In a Unity Connection cluster, the servers share the same phone system integrations. Each server is responsible for handling a share of the incoming calls for the cluster (answering phone calls and taking messages).

Depending on the phone system integration, each voice messaging port is either assigned to a specific server or used by both servers. Table 4-1 describes the port assignments.

Table 6: Server Assignments and Usage of Voice Messaging Ports in a Unity Connection Cluster

Integration Type	Server Assignments and Usage of Voice Messaging Ports
Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express	• The phone system is set up with twice the number of SCCP voicema that are needed to handle the voice messaging traffic. (For examp voicemail port devices are needed to handle all voice messaging t voicemail port devices must be set up on the phone system.) • In Cisco Unity Connection Administration, the voice messaging p configured so that half the number of the ports set up on the phon assigned to each server in the cluster. (For example, each server i has 16 voice messaging ports.) • On the phone system, a line group, hunt list, and hunt group are c enable the subscriber server answer most of the incoming calls fo • If one of the servers stops functioning (for example, when it is sh maintenance), the remaining server assumes responsibility of han incoming calls for the cluster. • When the server that stopped functioning is able to resume its nor and is activated, it resumes the responsibility of handling its share calls for the cluster.
Integration through a SIP Trunk with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express	• In Cisco Unity Connection Administration, half the number of vo ports that are needed to handle voice messaging traffic are assigned in the cluster. (For example, if 16 voice messaging ports are need all voice messaging traffic for the cluster, each server in the cluste 8 voice messaging ports.) • On the phone system, a route group, route list, and route pattern a to distribute calls equally between both servers in the cluster. • If one of the servers stops functioning (for example, when it is sh maintenance), the remaining server assumes responsibility of han incoming calls for the cluster. • When the server that stopped functioning is able to resume its nor and is activated, it resumes responsibility of handling its share of i for the cluster.

Integration Type	Server Assignments and Usage of Voice Messaging Ports
Integration through PIMG/TIMG units	• The number of ports set up on the phone system is the same as the nu voice messaging ports on each server in the cluster so that the servers the voice messaging ports. (For example, if the phone system is set u voice messaging ports, each server in the cluster must have the same messaging ports.) • On the phone system, a hunt group is configured to distribute calls eq both servers in the cluster. • The PIMG/TIMG units are configured to balance the voice messagin between the servers. • If one of the servers stops functioning (for example, when it is shut d maintenance), the remaining server assumes responsibility of handlin incoming calls for the cluster. • When the server that stopped functioning is able to resume its norma and is activated, it resumes responsibility of handling its share of inco for the cluster.
Other integrations that use SIP	• In Cisco Unity Connection Administration, half the number of voice ports that are needed to handle voice messaging traffic are assigned to e in the cluster. (For example, if 16 voice messaging ports are needed t all voice messaging traffic for the cluster, each server in the cluster h messaging ports.) • On the phone system, a hunt group is configured to distribute calls eq both servers in the cluster. • If one of the servers stops functioning (for example, when it is shut d maintenance), the remaining server assumes responsibility of handlin incoming calls for the cluster. • When the server that stopped functioning is able to resume its normal it resumes responsibility of handling its share of incoming calls for th

Stopping All Ports from Taking New Calls

Follow the steps in this section to stop all the ports on a server from taking any new calls. Calls in progress continue until the callers hang up.

Tip Use the Port Monitor page in the Real-Time Monitoring Tool (RTMT) to determine whether any port is currently handling calls for the server. For more information, see the Step a

Stopping All Ports on a Unity Connection Server from Taking New Calls

Procedure

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 Expand the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Port Manager, in the Change Port Status column, select **Stop Taking Calls** for the server.

Restarting All Ports to Take Calls

Follow the steps in this section to restart all the ports on a Unity Connection server to allow them take calls again after they were stopped.

Procedure

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 Expand the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Port Manager, in the Change Port Status column, select **Take Calls** for the server.

Server Status and its Functions in a Unity Connection Cluster

Each server in the cluster has a status that appears on the Cluster Management page of Cisco Unity Connection Serviceability. The status indicates the functions that the server is currently performing in the cluster, as described in Table 4-2.

Table 7: Server Status in a Unity Connection Cluster

Server Status	Responsibilities of the Sever in a Unity Connection Cluster
Primary	• Publishes the database and message store both of which are replicated to the other server in t • Receives replicated data from the other server. • Displays and accepts changes to the administrative interfaces, such as Unity Connection Adm and Cisco Unified Operating System Administration. This data is replicated to the other ser cluster. • Answers phone calls and takes messages. • Sends message notifications and MWI requests. • Sends SMTP notifications and VPIM messages. • Synchronizes voice messages in Unity Connection and Exchange mailboxes if the unified m feature is configured. • Connects with the clients, such as email applications and the web tools available through Ci **Note** A server with Primary status cannot be deactivated.
Secondary	• Receives replicated data from the server with Primary status. Data includes the database and store. • Replicates data to the server with Primary status. • Displays and accepts changes to the administrative interfaces, such as Unity Connection Adm and Cisco Unified Operating System Administration. The data is replicated to the server wi status. • Answers phone calls and takes messages. • Connects with the clients, such as email applications and the web tools available through Ci **Note** Only a server with Secondary status can be deactivated.
Deactivated	• Receives replicated data from the server with Primary status. Data includes the database and store. • Does not display the administrative interfaces, such as Unity Connection Administration an Unified Operating System Administration. The data is replicated to the server with Primary • Does not answer phone calls or take messages. • Does not connect with the clients, such as email applications and the web tools available thr Cisco PCA.

Server Status	Responsibilities of the Sever in a Unity Connection Cluster
Not Functioning	• Does not receive replicated data from the server with Primary status. • Does not replicate data to the server with Primary status. • Does not display the administrative interfaces, such as Unity Connection Administration Unified Operating System Administration. • Does not answer phone calls or take messages. **Note** A server with Not Functioning status is usually shut down.
Starting	• Receives replicated database and message store from the server with Primary status. • Replicates data to the server with Primary status. • Does not answer phone calls or take messages. • Does not synchronize voice messages between Unity Connection and Exchange mailbox inbox). **Note** This status lasts only a few minutes, after which the server takes the applicable status.
Replicating Data	• Sends and receives data from the cluster. • Does not answer phone calls or take messages for sometime. • Does not connect with clients, such as email applications and the web tools available thr Cisco PCA for sometime. **Note** This status lasts only a few minutes, after which the previous status resumes for the server.
Split Brain Recovery (*After detecting two servers with Primary status)*	• Updates the database and message store on the server that is determined to have Primary • Replicates data to the other server. • Does not answer phone calls or take messages for sometime. • Does not synchronize voice messages between Unity Connection and Exchange mailbox inbox is turned on for sometime. • Does not connect with clients, such as email applications and the web tools available thr Cisco PCA for sometime. **Note** This status lasts only a few minutes, after which the previous status resumes for the server.

Changing Server Status in a Cluster and its Effects

The Unity Connection cluster status can be changed either automatically or manually.

You can manually change the status of servers in a cluster in the following ways:

1. A server with Secondary status can be manually changed to Primary status. See the Manually Changing the Server Status from Secondary to Primary section.
2. A server with Secondary status can be manually changed to Deactivated status. See the Manually Activating a Server with Deactivated Status.
3. A server with Deactivated status can be manually activated so that its status changes to Primary or Secondary, depending on the status of the other server. See the Manually Activating a Server with Deactivated Status section.

Manually Changing the Server Status from Secondary to Primary

Procedure

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 From the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, from the Server Manager menu, in the Change Server Status column of the server with Secondary status, select **Make Primary**.

Step 4 When prompted to confirm the change in server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Note
The server that originally had Primary status automatically changes to Secondary status.

Manually Changing from the Server Status from Secondary to Deactivated

Procedure

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 From the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, select the server with Secondary status.

Step 4 In the right pane, select **Start Polling**. Note whether any voice messaging ports are currently handling calls for the server.

Step 5 Sign in to Cisco Unity Connection Serviceability.

Step 6 From the Tools menu, select **Cluster Management**.

Step 7 If no voice messaging ports are currently handling calls for the server, skip to Step 8.

If there are voice messaging ports that are currently handling calls for the server, on the Cluster Management page, in the Change Port Status column, select **Stop Taking Calls** for the server and then wait until RTMT shows that all ports for the server are idle.

Step 8 On the Cluster Management page, from the Server Manager menu, in the Change Server Status column for the server with Secondary status, select **Deactivate**.

Deactivating a server terminates all the calls that the ports for the server are handling.

Step 9 When prompted to confirm the change in the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Manually Activating a Server with Deactivated Status

Procedure

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 From the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, in the Server Manager menu, in the Change Server Status column for the server with Deactivated status, select **Activate**.

Step 4 When prompted to confirm the change in the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Effect on Calls in Progress When Server Status Changes in a Unity Connection Cluster

When the status of a Unity Connection server changes, the effect on calls in progress depend upon the final status of the server that is handling a call and on the condition of the network. The following table describes the effects:

Table 8: Effect on Calls in Progress When Server Status Changes in a Unity Connection Cluster

Status Change	Effects
Primary to Secondary	When the status change is initiated manually, calls in progress are not affected. When the status change is automatic, effect on calls in progress depend on the critical service that stopped.
Secondary to Primary	When the status change is initiated manually, calls in progress are not affected. When the status change is automatic, effect on calls in progress depend upon the critical service that stopped.

Status Change	Effects
Secondary to Deactivated	Calls in progress are dropped. To prevent dropped calls, on the Cluster Management page in Cisco Unity Connection Serviceability, select Stop Taking Calls for the server and wait until all the calls get ended and deactivate the server.
Primary or Secondary to Replicating Data	Calls in progress are not affected.
Primary or Secondary to Split Brain Recovery	Calls in progress are not affected.

If network connections are lost, then calls in progress may be dropped depending upon the nature of the network problem.

Effect on Unity Connection Web Applications When the Server Status Changes

The functioning of the following web applications is not affected when the server status changes:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unity Connection web tools accessed through the Cisco PCA—the Messaging Assistant, Messaging Inbox, and Personal Call Transfer Rules web tools
- Cisco Web Inbox
- Representational state transfer (REST) API clients

Effect of Stopping a Critical Service on a Unity Connection Cluster

Critical services are necessary for the normal functioning of the Unity Connection system. The effects of stopping a critical service depend upon the server and its status described in the following table:

Table 9: Effects of Stopping a Critical Service on a Unity Connection Cluster

Server	Effects
Publisher	• When the server has Primary status, stopping a critical service in Cisco Unity Connection Serviceability causes the server status to change to Secondary and degrades the ability of the server to function normally. The status of the subscriber server changes to Primary if it does not have the Disabled or Not Functioning status. • When the server has Secondary status, stopping a critical service in Cisco Unity Connection Serviceability degrades the ability of the server to function normally. The status of the servers does not change.
Subscriber	When the server has Primary status, stopping a critical service in Cisco Unity Connection Serviceability degrades the ability of the server to function normally. The status of the servers does not change.

Shutting Down a Server in a Cluster

When a Unity Connection server has Primary or Secondary status, it is handles voice messaging traffic and cluster data replication. We do not recommend you to shutdown both the servers in a cluster at the same time to avoid abrupt termination of the calls and replication that are in progress.

Consider the following points when you want to shutdown a server in a Unity Connection cluster:

- Shutdown the server during non business hours when voice messaging traffic is low.
- Change the server status from Primary or Secondary to Deactivated before shutting down.

Procedure

Step 1 On the server that does not shut down, sign in to Cisco Unity Connection Serviceability.

Step 2 From the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, locate the server that you want to shut down.

Step 4 If the server that you want to shut down has Secondary status, skip to Step 5.

If the server that you want to shut down has Primary status, change the status:

a) In the Change Server Status column for the server with Secondary status, select **Make Primary**.
b) When prompted to confirm the change in the server status, select **OK**.
c) Confirm that the Server Status column indicates that the server has Primary status now and that the server you want to shut down has Secondary status.

Step 5 On the server with Secondary status (the one you want to shut down), change the status:

a) Sign in to the Real-Time Monitoring Tool (RTMT).
b) From the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.
c) In the Node field, select the server with Secondary status.
d) In the right pane, select **Start Polling**.
e) Note whether any voice messaging ports are currently handling calls for the server.
f) If no voice messaging ports are currently handling calls for the server, skip to Step5g..

   If there are voice messaging ports that are currently handling calls for the server, on the Cluster Management page, in the Change Port Status column, select **Stop Taking Calls** for the server and then wait until RTMT shows that all ports for the server are idle.

g) On the Cluster Management page, from the Server Manager menu, in the Change Server Status column for the server with Secondary status, select **Deactivate**.

   Caution
   Deactivating a server terminates all calls that the ports for the server are handling.

h) When prompted to confirm the change in the server status, select **OK**.
i) Confirm that the Server Status column indicates that the server now has Deactivated status.

Step 6 Shut down the server that you deactivated:

a) Sign in to Cisco Unity Connection Serviceability.
b) Expand Tools and select Cluster Management.

c) Make sure that the Server Status column shows Not Functioning status for the server that you shutdown.

Replacing Servers in a Cluster

Follow the steps in the given sections to replace publisher or subscriber server in a cluster:

- To replace the publisher server, see the Replacing a Publisher Server section.
- To replace the subscriber server, see the Replacing a Subscriber Server section.

How a Unity Connection Cluster Works

The Unity Connection cluster feature provides high availability voice messaging through two Unity Connection servers that are configured in a cluster.

The Unity Connection cluster behavior when both the servers are active:

- The cluster can be assigned a DNS name that is shared by the Unity Connection servers.
- Clients, such as email applications and the web tools available through the Cisco Personal Communications Assistant (PCA) can connect to either of the Unity Connection server.
- Phone systems can send calls to either of the Unity Connection server.
- Incoming phone traffic load is balanced between the Unity Connection servers by the phone system, PIMG/TIMG units, or other gateways that are required for the phone system integration.

Each server in a cluster is responsible for handling a share of the incoming calls for the cluster (answering phone calls and taking messages). The server with Primary status is responsible for the following functions:

- Homing and publishing the database and message store that are replicated to the other server.
- Sending message notifications and MWI requests (the Connection Notifier service is activated).
- Sending SMTP notifications and VPIM messages (the Connection Message Transfer Agent service is activated).
- Synchronizing voice messages between Unity Connection and Exchange mailboxes, if the unified messaging feature is configured (the Unity Connection Mailbox Sync service is activated).

When one of the servers stops functioning (for example, when it is shutdown for maintenance), the remaining server resumes the responsibility of handling all the incoming calls for the cluster. The database and message store are replicated to the other server when its functionality is restored.

When the server that stopped functioning is able to resume its normal functions and is activated, it resumes responsibility of handling its share of incoming calls for the cluster.

Note It is recommended to perform provisioning only on the Publisher server in Active-Active mode and on Subscriber (Acting Primary) in case of cluster failover. The password change and password setting modification for User PIN/Web application should be provisioned on Publisher server in Active-Active mode.

To monitor the server status, the Connection Server Role Manager service runs in Cisco Unity Connection Serviceability on both the servers. This service performs the following functions:

- Starts the applicable services on each server, depending on server status.
- Determines whether critical processes (such as voice message processing, database replication, voice message synchronization with Exchange, and message store replication) are functioning normally.
- Initiates changes to server status when the server with Primary status is not functioning or when critical services are not running.

Note the following limitations when the publisher server is not functioning:

- If the Unity Connection cluster is integrated with an LDAP directory, directory synchronization does not occur, although authentication continues to work when only the subscriber server is functioning. When the publisher server is resumes functioning, directory synchronization also resumes.
- If a digital or HTTPS network includes the Unity Connection cluster, directory updates do not occur, although messages continue to be sent to and from the cluster when only the subscriber server is functioning. When the publisher server is functioning again, directory updates resume.

The Connection Server Role Manager service sends a keep-alive events between the publisher and subscriber servers to confirm that the servers are functioning and connected. If one of the servers stops functioning or the connection between the servers is lost, the Connection Server Role Manager service waits for the keep-alive events and may require 30 to 60 seconds to detect that the other server is not available. While the Connection Server Role Manager service is waiting for the keep-alive events, users signing in to the server with Secondary status are not able to access their mailbox or send messages, because the Connection Server Role Manager service has not yet detected that the server with Primary status (which has the active message store) is unavailable. In this situation, callers who attempt to leave a message may hear dead air or may not hear the recording beep.

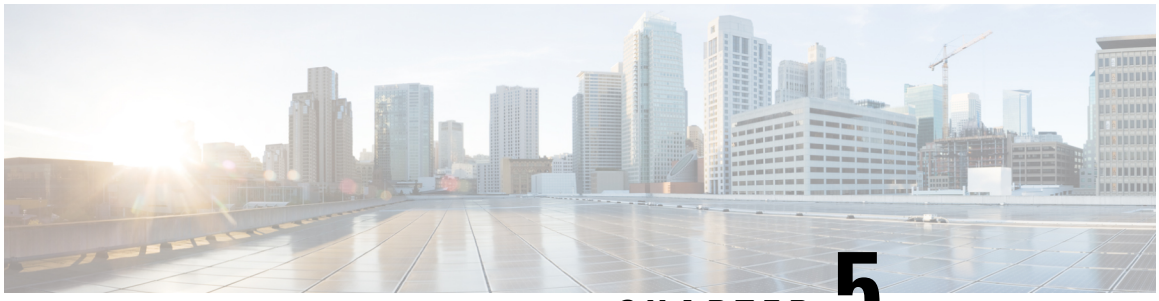
Note It is recommended to import and delete the LDAP users from the publisher node only.

Effects of Split Brain Condition in a Unity Connection Cluster

When both the servers in a Unity Connection cluster have Primary status at the same time (for example, when the servers have lost their connection with each other), both servers handle the incoming calls (answer phone calls and take messages), send message notifications, send MWI requests, accept changes to the administrative interfaces (such as Unity Connection Administration), and synchronize voice messages in Unity Connection and Exchange mailboxes if single inbox is turned on. However, the servers do not replicate the database and message store to each other and do not receive replicated data from each other.

When the connection between the servers is restored, the status of the servers temporarily changes to Split Brain Recovery while the data is replicated between the servers and MWI settings are coordinated. During the time when the server status is Split Brain Recovery, the Connection Message Transfer Agent service and the Connection Notifier service (in Cisco Unity Connection Serviceability) are stopped on both servers, so Unity Connection does not deliver any messages and does not send any message notifications. The Connection Mailbox Sync service is also stopped, so Unity Connection does not synchronize voice messages with Exchange (single inbox). The message stores are also briefly dismounted, so that Unity Connection tells users who are trying to retrieve their messages at this point that their mailboxes are temporarily unavailable.

When the recovery process is complete, the Connection Message Transfer Agent service and the Connection Notifier service are started on the publisher server. Delivery of the messages that arrived while during the recovery process may take additional time, depending on the number of messages to be delivered. The Connection Message Transfer Agent service and the Connection Notifier service are started on the subscriber server. Finally, the publisher server has Primary status and the subscriber server has Secondary status. At this point, the Connection Mailbox Sync service is started on the server with Primary status, so that Unity Connection can resume synchronizing voice messages with Exchange if single inbox is turned on.



CHAPTER 5

Maintaining Cisco Unity Connection Server

- Migrating a Physical Server to a Virtual Machine, on page 75
- Replacing the Non-Functional Server, on page 78
- Changing the IP Address or Hostname of a Unity Connection Server, on page 79
- Adding or Removing Unity Connection Languages, on page 83
- Removing Unity Connection Language Files, on page 86

Migrating a Physical Server to a Virtual Machine

Follow the given tasks to migrate from physical server to a virtual machine:

- Backup the software component on the physical server. For more information, see the Backing Up and Restoring Cisco Unity Connection Components chapter.
- Download and deploy the OVA template to create a new virtual machine. For more information, see the Creating a Virtual Machine section.
- Migrating the Unity Connection server on the virtual machine.
  - To replace the publisher server, see the Replacing a Publisher Server section.
  - To replace the subscriber server, see the Replacing a Subscriber Server section.
- If Unity Connection is installed as a standalone server, restore the software component from the physical server to the virtual machine for which you have taken the back up. For more information, see the Restoring the Software Components on Unity Connection section.
- (Optional) Install new languages on the replaced server if required or remove the existing languages already installed on the server. For more information, see the Adding or Removing Unity Connection Languages section.

Note If you are deploying Unity Connection networking (Intersite, Intrasite, or HTTPS), see the Networking Guide for Cisco Unity Connection, Release 14, before replacing the Unity Connection server, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/networking/guide/b_14cucnetx.html .

Replacing a Publisher Server

While you are upgrading the publisher server in a Unity Connection cluster, the subscriber server continues to provide services to the users and callers.

Note In case of a standalone server, replace the server during off-peak hours to avoid call-processing interruptions and impact to services.

Procedure

Step 1 Manually change the status of subscriber server to Primary:

a) Sign in to Cisco Unity Connection Serviceability.
b) Expand Tools and select Cluster Management.
c) On the Cluster Management page, from the Server Manager menu, locate the subscriber server and check the following:

- If the subscriber server status is Primary, skip the remaining steps in this procedure.
- If the subscriber server status is Secondary, select Make Primary.
- If the subscriber has Deactivated status, change the status to Secondary and then select Activate. When prompted to confirm changing the server status, select OK. After successful activation of the subscriber server, change the status to Primary selecting Make Primary option.

Step 2 Manually change the status of publisher server to Deactivated:

a) Sign in to the Real-Time Monitoring Tool and select Port Monitor.
b) In the Node field, select the publisher server and then select Start Polling. Note whether any voice messaging ports are currently handling calls for the server.
c) Return to the Cluster Management page of Cisco Unity Connection Serviceability and do any one of th following:

- If no voice messaging ports are currently handling calls for the publisher server, move to the next 3.
- If there are voice messaging ports that are currently handling calls for the publisher server, on the Cluster Management page, in the Port Manager column, select Stop Taking Calls for the publisher server and then wait until RTMT shows that all the ports for the publisher server are idle.

d) From the Server Manager menu, in the Change Server Status column for the publisher server, select Deactivate and then select OK.

Step 3 Install the replacement publisher server, see Installing the Publisher Server section.

a) Shut down the publisher server using the CLI command utils system shutdown. On the Cluster Management page of the subscriber server, the publisher has Not Functioning status.
b) Install the virtual machine. The following settings on the virtual machine must be same as that on the physical server, otherwise the transfer of data from the physical server to the virtual machine get failed:

- Hostname of the server
- IP address of the server
- Time zone

- NTP server
- DHCP settings
- Primary DNS settings
- SMTP hostname
- X.509 Certificate information (Organization, Unit, Location, State, and Country).

Step 4 You must run the utils disaster_recovery prepare restore pub_from_sub CLI command on the publisher server. This command handles the tasks to prepare for restore of a publisher node from a subscriber node.

Step 5 Configure the cluster on the replaced publisher server:

a) Sign in to Cisco Unity Connection Administration on the publisher server.
b) Expand System Settings and select Cluster.
c) On the Find and List Servers page, select Add New.
d) On the New Server Configuration page, in the Hostname/IP Address field, enter the hostname or IP address of the subscriber server. Enter the description and select Save.

Step 6 If Unity Connection is installed as a cluster, you can restore the publisher using the subscriber data.

a) Run the utils cuc cluster renegotiate CLI command on the subscriber server. The publisher automatically restarts after running this command.
b) Run the show cuc cluster status CLI command on the subscriber server to confirm that the new Unity Connection cluster is configured correctly.

Note
If third-party certificates are deployed in Unity Connection then after successfully replacing the publisher server, you must reconfigure third party certificates for the newly build publisher server. For information on how to configure the certificates, see Security chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html.

Replacing a Subscriber Server

While you are upgrading the subscriber server in a Unity Connection cluster, the publisher server continues to provide services to users and callers.

Procedure

Step 1 Manually change the status of publisher server to Primary:

a) Sign in to Cisco Unity Connection Serviceability.
b) Expand Tools and select Cluster Management.
c) On the Cluster Management page, from the Server Manager menu, locate the publisher server and check the following:

- If the publisher server status is Primary, skip the remaining steps in this procedure.
- If the publisher server status is Secondary, change the status by selecting Make Primary.

- If the publisher has Deactivated status, change the status to Secondary and select Activate. A prompt appears to confirm the changing of the server status, select OK. After successful activation of the publisher server, change the status to Primary by selecting Make Primary option.

Step 2 Manually change the status of subscriber server to Deactivated:

a) Sign in to the Real-Time Monitoring Tool, expand <Unity Connection> option and select Port Monitor.

b) In the Node field, select the subscriber server and select Start Polling. Note whether any voice messaging ports are currently handling calls for the server.

c) Return to the Cluster Management page of Cisco Unity Connection Serviceability.

- If no voice messaging ports are currently handling calls for the server, skip to the next step.
- If there are voice messaging ports that are currently handling calls for the subscriber server, on the Cluster Management page, in the Change Port Status column, select Stop Taking Calls for the subscriber server and then wait until RTMT shows that all ports for the server are idle.

d) From the Server Manager menu, in the Change Server Status column for the subscriber server, select Deactivate and select OK.

Step 3 Make sure that the hostname or IP address of the subscriber server is configured correctly on the publisher server as mentioned in 4 of replacing a publisher server.

Step 4 Install the replaced subscriber server, see Installing the Publisher Server section.

a) Shut down the subscriber server using the CLI command utils system shutdown. On the Cluster Management page of the publisher server, the subscriber has Not Functioning status.

b) Reinstall the Unity Connection server. You must specify the same security password of the subscriber server that you are replacing and it should also match the security password for the publisher server. Otherwise, the Unity Connection cluster do not function. If you do not know the security password, you can change it on the publisher server before you install the subscriber server using the CLI command set password user.

Step 5 Check the cluster status by running the show cuc cluster status CLI command on the subscriber server.

Note

a. If third-party certificates are deployed in Unity Connection then after successfully replacing the subscriber server, you must reconfigure third party certificates for the newly build subscriber server. For information on how to configure the certificates, see Security chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx/b_14cucosagx_chapter_0101.html.

b. *(Applicable to 14 SU4 or later)* If you are using SpeechView with Cisco Webex in-house transcription service, onboard the Subscriber Server of the Unity Connection Cluster on Cisco Webex Cloud-Connected UC. For more details on Onboarding Unity Connection server on Cisco Webex Cloud-Connected UC, refer https://help.webex.com/en-us/article/nzt6c0b/Set-up-Webex-Cloud-Connected-UC-for-on-premises-devices.

Replacing the Non-Functional Server

Replacing the Non-Functional Server

Tasks	Procedure
If Unity Connection is installed as standalone.	• Recreate the virtual machine. For more information, see the Creating a Virtual Machine section. • Restore the software. For more information, see the Restoring the Software Components on Unity Connection section.
If Unity Connection is installed as a cluster and publisher is not functioning.	• Recreate the virtual machine. For more information, see the Creating a Virtual Machine section. • Replace the Publisher server, see the Replacing a Publisher Server section.
If Unity Connection is installed as a cluster and subscriber is not functioning.	Install the subscriber server, see the Installing the Subscriber Server section.

If both the servers are not functioning in a cluster.	• Replace the publisher server, see Installing the Publisher Server section.
	• Restore the software components on the physical machine. For more information, see the Restoring the Software Components on Unity Connection section.
	• Configure cluster on the publisher sever:
	  • Replace the subscriber server, see the Installing the Subscriber Server section.
	  • Check the cluster status using CLI command show cuc cluster status.
	  • Synchronize MWIs on each phone system.

Changing the IP Address or Hostname of a Unity Connection Server

Before changing the IP address of a standalone Unity Connection server or a cluster, you need to determine whether the server is defined by hostname or IP address.

Note You can also use Cisco Prime Collaboration Deployment for readdressing. For more information on Cisco PCD, see http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.

Determine Whether Unity Connection is Defined by Hostname or IP Address

Procedure

Step 1 Sign in to Cisco Unity Connection Administration of the server of which the IP address needs to be changed.

Step 2 Expand System Settings and select Cluster.

Note
You need to select Cluster even if you want to change the IP address or hostname of a standalone server.

Step 3 Select Find to locate the server of which you need to change the IP address or hostname:

- If the value of the Hostname/IP Address column is a hostname, the server is defined by a hostname.
- If the value of the Hostname/IP Address column is an IP address, the server is defined by an IP address.

Important Considerations before Changing the Hostname or IP Address of a Unity Connection Server

1. When you change the IP address or hostname of the Unity Connection server, make sure to apply the same changes on all the associated components that refer the Unity Connection server by IP address or hostname:
2. Bookmarks on client computers to the following web applications:
   - Web applications, such as Cisco Personal Communications Assistant and Cisco Unity Connection Administration.
   - Cisco Fax Server
   - Cisco Unified Application Environment
   - Cisco Unified Mobile Advantage
   - Cisco Unified Presence
   - Cisco Unified Personal Communicator
   - Cisco Unity Connection ViewMail for Microsoft Outlook
   - IMAP email clients that access Unity Connection
   - Phone systems and related components, including Cisco EGW 2200, Cisco ISR voice gateway, Cisco SIP Proxy Server, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and PIMG/TIMG units.
   - RSS readers
   - SMTP smart host

- Voice messaging systems with which Unity Connection is integrated via VPIM, such as Cisco Unity and Cisco Unity Express.

Caution If associated components reference the Unity Connection server by IP address and if you do not change the IP address as applicable, the components are no longer be able to access Unity Connection.

3. You can change the IP address and hostname of a Unity Connection server or cluster following the steps mentioned in the Changing the IP Address or Hostname of a Unity Connection Server or Cluster section.

Caution Do not change the IP address or hostname of a Unity Connection server during business hours.

4. (Only in case of changing IP address of a Unity Connection server) If the Unity Connection server is configured to get an IP address from a DHCP server, you cannot manually change the IP address of the server. Instead, you must do one of the following:
   - Change DHCP/DNS settings from Cisco Unified Operating System Administration> Settings and select the applicable option from IP, and restart Unity Connection by running the CLI command utils system restart.
   - Disable DHCP on Unity Connection by running the CLI command set network dhcp and then manually change the IP address by doing the procedure given below.

Note To change the IP address or hostname of a Unity Connection cluster, follow the steps mentioned in the Changing the IP Address or Hostname of a Unity Connection Server section first on the publisher server and then on the subscriber server.

Changing the IP Address or Hostname of a Unity Connection Server or Cluster

Note We can also change IP Address or Hostname of Cisco Unity Connection standalone node or cluster using CLI . For more information on CLI usage see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/14SU2/cucm_b_cli_reference_guide_release_14su2/cucm_b_cli_reference_guide_release_1401_chapter_0110.html#CUCM_CL_SEB8A06A_00

Do the following steps to change the IP address or Hostname of a standalone server or a cluster defined by hostname or IP address using GUI. In case of a cluster, follow the steps first on the publisher server and then on the subscriber server.

Procedure

Step 1 Sign in to the standalone server or the publisher server using Real-Time Monitoring Tool. Expand Tools> Alert and select Alert Central. In the Systems tab, make sure the ServerDown is black. If ServerDown is red, then resolve all the problems and change it to black.

Step 2 Check the server status:

a) Sign in to Cisco Unity Connection Serviceability.
b) Expand Tools and select Cluster Management.
c) On the Cluster Management page, check whether server status is Primary or Secondary. If there is any other status value then resolve the problem.

Step 3 Check the network connectivity and DNS server configuration by running the utils diagnose module validate_network CLI command.

Step 4 Backup the database using Disaster Recovery System. See the Backing Up and Restoring Cisco Unity Connection Components chapter.

Step 5 If intrasite, HTTPS, and SRSV networking is configured, remove the server from the Unity Connection site. For instructions, see the Networking Guide for Cisco Unity Connection, Release 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/networking/guide/b_14cucnetx.html.

Caution
Re-adding a server to a Unity Connection site can be a time consuming process.

Step 6 On a DNS server, change the DNS record of the Unity Connection server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 7 *(Applicable only when you change the IP address or Hostname of a standalone server or a cluster defined by an IP address or Hostname)* Changing the IP addresses or Hostname of a standalone server or the publisher server in Connection Administration:

a) Sign in to Cisco Unity Connection Administration.

Caution
In case of a cluster, you must sign in to the publisher sever and select subscriber server to change the IP address or Hostname of a subscriber server.

b) Expand System Settings, and select Cluster.
c) Select Find to display a list of servers in the cluster.
d) Select the name of the standalone server or publisher server.
e) Change the value of the Hostname/IP Address field to the new Hostname/IP address.
f) Select Save.

Step 8 On the standalone or publisher server, change the IP address, Hostname, and default gateway (if applicable):

a) Sign in to Cisco Unified Operating System Administration.
b) From the Settings menu, select **IP** > **Ethernet**.
c) In the Host Information, enter the value of Hostname.
d) If you want an alternate hostname for the server, run the **set web-security** CLI command. In the Hostname, change the hostname of the server.

For more information on the CLI commands, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html .

Note
Enter a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA).

(In case of SSL certificates created and installed on renamed server) Upload the root certificate and the server certificate to the standalone or publisher server. Follow the steps as mentioned in Security Guide for Cisco Unity Connection Release 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

e) In the Port Information, change the value of the IP Address and Subnet Mask field (if applicable).
f) If you are moving the server to a different subnet that requires a new default gateway address, change the value of the Default Gateway field in the Gateway Information.
g) Select Save.

Caution
After saving the page, node services will restart automatically. Restarting services ensures the proper update for the changes to take effect. Do not perform any action on the server until the services are up and running. To check the status of the services, run **utils service list** CLI command.

Step 9 If you change the IP address or Hostname of a standalone server, skip to Step 10.

(Applicable only when you change the IP address or Hostname of a publisher server in case of a cluster) On the subscriber server, change the IP address of the publisher server:

a) Sign in to Cisco Unified Operating System Administration.
b) From the Settings menu, select IP > Publisher.
c) Change the IP address of the publisher server.
d) Select Save.

Step 10 Sign in to Real-Time Monitoring Tool and confirm that the server is available and running.

This completes the process of changing the IP address of the standalone server.

Step 11 For the cluster, repeat Step 1 to Step 9 on subscriber server also.

This completes the process of changing the IP address of a cluster.

Adding or Removing Unity Connection Languages

After installing a new server or on an existing server, you may need to add some new language(s) and remove some already installed languages depending on the user requirement.

Note Languages are not licensed and Unity Connection 14 does not enforce a limit on the number of languages you can install and use. However, the more languages you install, the less hard disk space is available for storing voice messages.

Task List for Adding Languages to a Standalone Unity Connection Server

Do the following tasks to download and install languages in addition to English (United States):

1. Download the Unity Connection languages that you want to install and do the following steps:
   a. Sign in as a registered user on the following Cisco.com link: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240.
   b. Expand **Unified Communications Applications > Voicemail and Unified Messaging > Cisco Unity Connection**, and select the applicable Unity Connection version.
   c. On the Select a Software Type page, select **Cisco Unity Connection Locale Installer**.
   d. On the Select a Release page, select the applicable Unity Connection version. The download links for the languages appear on the right side of the page.
   e. Select the name of a file to download. On the Download Image page, note down the MD5 value and follow the on screen prompts to complete the download.

Note Make sure that the MD5 checksum matches the checksum that is listed on Cisco.com. If the values do not match, the downloaded file is damaged. Do not attempt to use a damaged file to install software as the results is unpredictable. If the MD5 values do not match, download the file again until the value for the downloaded file matches the value listed on Cisco.com.

2. (Unity Connection cluster only) Make sure that the subscriber server status is Primary and the publisher server status is Secondary in order to install the Unity Connection languages. Follow the given steps:
   a. Sign in to Cisco Unity Connection Serviceability.
   b. Expand Tools and select Cluster Management.
   c. For subscriber server, select Make Primary.
3. On the standalone or publisher server, install the Unity Connection languages that you downloaded. Refer Installing Unity Connection Language Files from Network Location or Remote Server for more details.
4. If you are using additional languages because you want the Cisco Personal Communications Assistant to be localized: Download and install the corresponding Unity Connection locales on the publisher server.
5. (Unity Connection cluster only) Change the publisher server status to Primary and follow the same steps on subscriber server to install the same Unity Connection languages that were installed on publisher server.

Installing Unity Connection Language Files from Network Location or Remote Server

In this procedure, do not use the web browser controls (for example, Refresh/Reload) while accessing Cisco Unified Operating System Administration. However, you can use the navigation controls in the administration interface.

Procedure

Step 1 Stop the Connection Conversation Manager and Connection Mixer services:

a) Sign in to Cisco Unity Connection Serviceability. Expand Tools menu and select **Service Management**.
b) In Critical Services, for the Connection Conversation Manager row, select **Stop**.
c) Wait for the service to stop.
d) In the Critical Services menu, in the Connection Mixer row, select **Stop**.
e) Wait for the service to stop.

Step 2 Sign in to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, select **Install/Upgrade**. The Software Installation/Upgrade window appears.

Step 4 In the Source list, select **Remote Filesystem**.

Step 5 In the Directory field, enter the path of the folder that contains the language file on the remote system.

If the language file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the folder path. (For example, if the language file is in the languages folder, you must enter **/languages**.)

If the language file is located on a Windows server, make sure that you are connecting to an FTP or SFTP server, and use the appropriate syntax:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root folder on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

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

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

Step 9 In the **Transfer Protocol** list, select the applicable option.

Step 10 Select **Next**.

Step 11 Select the language that you want to install, and select **Next**.

Step 12 Monitor the progress of the download.

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

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

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

Step 13 *If you want to install another language,*ct **Install Another**, and repeat all the above steps

Step 14 *If you are finished with installing languages:* Restart the services:

- Sign in to Cisco Unity Connection Serviceability.
- Expand Tools menu and select **Service Management**.
- In the Critical Services menu, in the Connection Conversation Manager row, select **Start**. Wait for the service to start.
- In the Critical Services menu, in the Connection Mixer row, select **Start**. Wait for the service to start.

Note

To complete the locale update, restart the Cisco Tomcat service across the entire cluster (both publisher and subscriber nodes). This ensures that the Cisco Unity Connection GUI is synchronized and that the correct language settings are displayed on both the publisher and subscriber nodes.

Removing Unity Connection Language Files

Procedure

Step 1 Sign in to the command line interface as a platform administrator.

Note
Make sure to stop Connection Conversation Manager and Connection Mixer services before uninstalling the languages.

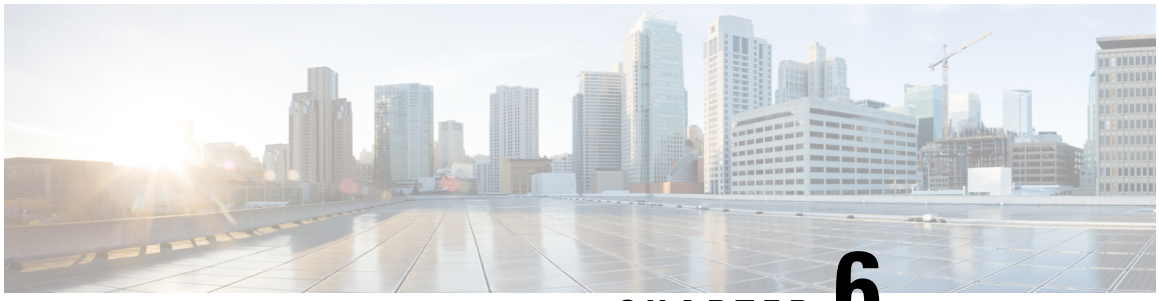
Step 2 Run the **show cuc locales** CLI command to display a list of installed language files.

Step 3 In the command results, find the language that you want to remove, and note the value of the Locale column for the language.

Step 4 Run the **delete cuc locale <code** > CLI command to remove the language, where <code> is the value of the Locale column that you get in Step 3.

When the command completes, the following information appears:

<code> uninstalled



CHAPTER 6

Managing Licenses

- Managing Licenses, on page 87

Managing Licenses

Overview

Unity Connection supports **Cisco Smart Software Licensing** which is simple and enhanced way for using various licensed features.Using Cisco Smart Software Licensing, you can manage all the licenses associated with an organization through **Cisco Smart Software Manager (CSSM)** or **Cisco Smart Software Manager satellite**. Cisco Smart Software Licensing establishes a pool of licenses or entitlements that can be used across your organization in a flexible and automated manner. This model of licensing provides the visibility of your licenses ownership and consumption. Unity Connection must be registered with the CSSM to use various licensed feature.

Cisco Smart Software Manager enables you to manage all of your Cisco Smart Software Licenses from one centralized website. You can use Cisco Smart Software Manager to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

For more information about Cisco Smart Software Manager, see https://software.cisco.com/

Cisco Smart Software Manager satellite is a component of Cisco Smart Software Licensing that manages product registrations and monitoring of smart license usage for Cisco products. If you do not want to manage Cisco products directly using Cisco Smart Software Manager, either for policy or network availability reasons, you can choose to install the Cisco Smart Software Manager satellite on-premises. Products register and report license consumption to the Cisco Smart Software Manager satellite as it does on Cisco Smart Software Manager.

For more information about the Cisco Smart Software Manager satellite, see http://www.cisco.com/web/ordering/smart-software-manager/smart-software-manager-satellite.html.

Note Cisco Smart Software Licensing is only the way to manage the licenses in Unity Connection.

For more information on Cisco Smart Software Licensing, see the "Smart Software Licensing Overview" available at, http://www.cisco.com/web/ordering/smart-software-licensing/index.html

Deployment Options

To view and manage the licenses, Unity Connection must communicate with the Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite.

Following are the options to deploy the Cisco Smart Software Licensing in Unity Connection, listed in an order from easiest to use to most secure:

- **Direct Cloud Access**: In this option, Unity Connection can directly communicate with CSSM and transfer the usage information over internet. No additional components are required.

Note In this option, Unity Connection must resolve the CSSM server directly through DNS.

- **Direct Cloud Access through an HTTPs Proxy**: In this option, Unity Connection directly transfers the usage information to CSSM over internet through proxy server.Administrator also provides an option to authenticate the proxy server for secure communication with CSSM. You can enter username and password for authentication of proxy server.
- **Mediated Access through an On-Premises Collector – Connected**: In this option, Unity Connection communicates with on-prem version of CSSM called Cisco Smart Software Manager satellite. Periodically satellite communicates with CSSM using Cisco network and exchange of license information will be performed to keep the databases in synch.
- **Mediated Access through an On-Premises Collector – Disconnected**: This option also uses the satellite that is not connected with Cisco network. For synchronization between satellite and CSSM, you will manually exchange the license information files to keep the database in synch.

Note License hierarchy is supported only with Cisco Smart Software Manager satellite version 6.0.0 and later.

To select the deployment options, see "Configuring Transport Setting" section.

Smart Account and Virtual Account

Smart Account is a simple and organized way to manage the product licenses and entitlements. Using this account, you can register, view, and manage your Cisco Software Licenses across your organization.

As per the organization requirements, you can create the sub accounts within your Smart Account. The sub accounts are known as Virtual Accounts that are collections of licenses and product instances. To manage the licenses, you can create multiple virtual accounts based on the different organization categories such as departments or locations. Virtual Accounts are maintained by Smart Account administrators. Licenses can be transferred within virtual accounts as per the requirement.

While moving product instance from one virtual account to another, the licenses assosiated with the previous virtual account are not transferred.

For more information on how to create and manage the Smart Account and Virtual Account, see "Cisco Smart Accounts" at http://www.cisco.com/web/ordering/smart-software-manager/smart-accounts.html

Prerequisites for Configuring Cisco Smart Software Licensing

To configure the Cisco Smart Software Licensing in Unity Connection, ensure the following requirements:

- Understand the Unified Communications (UC) licensing structure. For details, see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html.
- A Smart Account and Virtual Account must be created for Unity Connection. For more information, see "Smart Account and Virtual Account" section.

Note If you upgrade the Unity Connection from any earlier releases to 14, all the licenses(legacy and PLM based) used in Unity Connection must be migrated to the CSSM for using Cisco Smart Software Licensing. For more information, see "Migrating Licenses" section.

Configuring Cisco Smart Software Licensing in Unity Connection

By default, the Cisco Smart Software Licensing is enabled for Cisco Unity Connection. To use Cisco Smart Software Licensing, Unity Connection must register with CSSM or satellite. After fresh install, Unity Connection remains in Evaluation Mode until it is registered with CSSM or satellite. The Evaluation Period of 90 days are provided once in the entire life cycle of the product. As soon as Unity Connection consumes licenses, the Evaluation Period starts.

In Evaluation Mode, you cannot enable the encryption on Unity Connection. It means you are not allowed to use the security modules in Unity Connection. To enable the encryption in Unity Connection, you must register the product with CSSM or satellite using token that allows Export-Controlled Functionality. To enable the Export Controlled Functionality for the product, see "Token Creation" section.

After successfully registering the product with CSSM or satellite, run "utils cuc encryption enable" CLI command to enable the encryption on Unity Connection.

For more information on the CLI command, see the Command Line Interface Reference Guide for Cisco Unified Solutions for the latest release, available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

For more information on the encryption in Cisco Unity Connection, see "Cisco Unity Connection- Restricted and Unrestricted Version" chapter of the Security Guide for Cisco Unity Connection Release 14 available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

Note If data plane encryption (e.g. SRTP) has been turned on after registration to CSSM or satellite and the product is subsequently deregistered from CSSM or satellite, data plane encryption will continue to be enabled. An alarm will be sent warning the administer to disable data plane encryption when unregistered from CSSM or satellite. Data plane encryption will be disabled after a reboot of the product. Note that this encryption behavior, immediately after deregistration, may change in future versions of the product.

Configuring Transport Settings *(optional)*

To deploy the Cisco Smart Licensing in Unity Connection, you can configure the applicable transport settings. To configure the transport settings in Unity Connection, do the following procedure:

Procedure

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Licenses.

Step 2 On the Licenses page, select **View/Edit** link under Transport Settings field. A dialog box appears, on which select the applicable deployment option for the Smart Licensing. (For more information, see Help > This Page)

Step 3 Select Save.

Note By default, the Direct option is selected.

Token Creation

You must create a token to register the product with CSSM or satellite.

To create the token, do the following procedure:

Procedure

Step 1 Log in to your Smart Account in Cisco Smart Software Manager at software.cisco.com or Cisco Smart Software Manager satellite.

Step 2 Select the virtual account that contains the licenses for the product.

Step 3 In the General tab of virtual account, select New Token.

Step 4 In the Create Registration Token dialog box, enter the Description and Expire After information and select Create Token.

Step 5 To allow the Export Controlled Functionality for Unity Connection, check the **Allow export-controlled functionality on the products registered with this token** check box. By checking the check box, you can enable the encryption for the product registered with this Registration Token.

Note
The Smart Account that are entitled to use Export Controlled Functionality can only check the **Allow export-controlled functionality on the products registered with this token** check box.

Step 6 Once the token is created, copy the token to register the product.

For more information, see software.cisco.com

Registering the Unity Connection

To register the Unity Connection with CSSM or satellite, do the following procedure:

Procedure

Step 1 Log in to the Cisco Unity Connection Administration.

Step 2 Expand System Settings and select Licenses.

Step 3 On the Licenses page, select **Register** button. A dialog box appears, enter the registration token copied from the CSSM or satellite.

Step 4 Select **Register**.

Managing Cisco Smart Software Licensing

After successful registration of the Unity connection with CSSM or satellite , you can see the usage details on the Licenses page of the Cisco Unity Connection Administration. You can also manage the licenses by performing the various actions on Cisco Unity Connection Administration.

To perform the actions, go to Cisco Unity Connection Administration > System Settings > Licenses. On the Licenses page, select any one of the following from the Action menu:

- **Renew Authorization Now**: Using this option, you can manually renew the license authorization for all the licenses. However, the licenses are automatically authorized in every 6 hours.
- **Renew Registration Now**: After registering with CSSM or satellite, it provides a registration certificate to identify the product. This certificate is valid for one year. Using this option, you can manually renew the registration of the product. However, the registration of the product is automatically renewed in every six month.
- **Deregister**: Using this option, you can deregister the product from CSSM or satellite. All license entitlements used for the product are released back to its virtual account.
- **Reregister**: Using this option, you can reregister the product with CSSM or satellite.

Smart Software Licensing Status

Whenever Unity Connection communicates with the Cisco Smart Software Manager, there is a transition in the Unity Connection licensing status. The Smart Software Licensing Status provides an overview of license usage on the product.

The licensing status of the Unity Connection can be categorized as follows:

- **Registration Status**
- **Authorization Status**

Registration Status

The different registration status in a Unity Connection server are:

- **Unregistered**: The registration status of Unity Connection remains Unregistered until it successfully registers with CSSM or satellite.
- **Registered**: Unity Connection is successfully registered with CSSM or satellite.

- **Registration Expired**: The registration status of Unity Connection changes to the Registration Expired if registration of the product is not renewed within one year. After registration expired, the product goes back to the Evaluation Mode and you can use licenses for the remaining days of the Evaluation Period. When Evaluation Period of the product is expired and the product is still not registered with CSSM or satellite, you can not create or modify the users in Unity Connection.

Authorization Status

The different authorization status in a Unity Connection server are:

- **Evaluation Mode**: The authorization status of fresh installed Unity Connection is Evaluation Mode until it registers with CSSM or satellite. In this mode, Unity Connection can use licensed feature except SpeechView and SpeechViewPro. The Evaluation Period of 90 days are provided once in the entire life cycle of the product. The Evaluation Period of Unity Connection begins as soon as it starts consuming licenses. After successful registration with CSSM, the Evaluation timer stops. You can further use the remaining Evaluation Period when Unity Connection will go in Unregister or Registration Expired state.
- **Evaluation Period Expired**: if Unity Connection uses licenses for 90 days without registering with CSSM or satellite, the status of Unity Connection changes to Evaluation Period Expired. In this mode, user creation or modification are not allowed.
- **No Licenses in Use**: If Unity Connection does not use any licenses, the status changes to No License in Use.
- **Authorized**: In this state, all the licenses used by Unity Connection are authorized.
- **Out of Compliance**: Unity Connection authorization status changes to Out of Compliance either license usage exceeds the licenses available in the virtual account of the product or it uses the feature licenses that are not available in the virtual account.
- **Authorization Expired**: Unity Connection Authorization status changes to Authorization Expired if Unity Connection does not communicate with CSSM or satellite within the authorization time period of 90 days.

License Reservation in Unity Connection

Cisco Unity Connection provide the following license reservation features:

1. Unity Connection Release 12.5 and later, provides **Specific License Reservation** feature that allows the administrator to specify and reserve user licenses from the smart account and virtual account against a product instance. The product instance can use the reserved licenses without communicating usage information to CSSM.

Note In Specific License Reservation, reserved licenses of a virtual account are moved with the product instance.

2. Unity Connection Release 14SU1 and later, provides **Permanent License Reservation** feature that allows the administrator to reserve an entitled permanent license tag from the smart account and virtual account against a product instance.Administrators need to provision the User Licenses as needed by the Product instance in the Smart Account and Virtual Account. Once the registration has been successfully completed, the product will continue to remain in “authorized” state.

Note This feature is limted to FedRAMP customers. Permanent License Tag can be ordered through Cisco Commerce Workspace and will be provisioned in the Smart Account and Virtual Account after Cisco approval. For ordering, see *Cisco Collaboration Flex Plan 3.0 for FedRAMP Ordering Guide* available at https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/guide-c07-744596.html. After acquiring permanent licenses, customers should operate within the defined limits of license counts which they have purchased.

Configuring Specific License Reservation in Unity Connection

In Specific License Reservation, Unity Connection requires a manual exchange of information with CSSM for product configuration and authorization. To configure Specific License Reservation and perform its various functions, execute the CLI commands in the given below sequence:

- **license smart reservation enable**: This command is used to enable the license reservation feature.
- **license smart reservation request**: This command is used to generate reservation request code for Unity Connection.
- **license smart reservation install "<authorization code>"** or **license smart reservation install-file**: This command is used to install the license reservation authorization-code generated on the CSSM.

You can also perform additional operations by executing the given below CLI commands:

- **license smart reservation return**: This command is used to generate a return code. The return code must be entered into the CSSM to return the licenses to the virtual account.
- **license smart reservation cancel**: This command is used to cancel the reservation process before the authorization code obtained from CSSM against the product request code is installed.
- **license smart reservation return - authorization "<authorization code>"**: This command is used to generate a return code using the authorization code specified on the command line. The return code must be entered into the CSSM to return the licenses to the virtual account.

Note In case of a cluster, you can execute the CLI commands only on publisher server.

Configuring Permanent License Reservation in Unity Connection

In Permanent License Reservation, Unity Connection requires a manual exchange of information with CSSM for product configuration and authorization. To configure Permanent License Reservation and perform its various functions, execute the CLI commands in the section Configuring Specific License Reservation in Unity Connection, on page 93. These CLI commands are used for reserving Permanent License Tag.

Below mentioned CLI is specific to Permanent License Reservation:

- **license smart reservation set license_count**: This CLI command is used to specify or update the license count for the system to operate within, when set for Permanent License Reservation. License count set doesn't affect compliance status and is for administrator reference only.License count set can be referred on the License Management screen. Customers will operate within the defined limits of license counts which they have purchased.

If this CLI is not executed below warning message will be displayed on License Management screen.

"Administrator has not specified the license this system would operate within. Please run the CLI command "license smart reservation set license_count" and complete the Permanent License Reservation process."

Note If the customer purchases more licenses in future, administrator can update the purchased license count by running the CLI again.

For more information on above CLI commands, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 14* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

License Reservation Status

When Unity Connection manually exchanges information once with the CSSM, there is a transition in the Unity Connection license reservation status.

The licensing status for Specific License Reservation and Permanent License Reservation of the Unity Connection can be categorized as follows:

Registration Status

The different registration status for Specific License Reservation and Permanent License Reservation in a Unity Connection server are:

- **Unregistered**: The registration status of Unity Connection remains Unregistered until the product reservation request code has been generated.
- **Reservation In Progress**: When Unity Connection generates the reservation request code, the licensing status changes to Reservation in Progress.
- *(Applicable to Specific License Reservation only)* **Registered - Specific License Reservation**: When Unity Connection provides reservation request code to CSSM, CSSM generates an authorization code for the product. After successfully installing the authorization code on the product, the licensing status changes to Registered - Specific License Reservation.
- *(Applicable to Permanent License Resrvation only)* **Registered - Universal License Reservation**: When Unity Connection provides reservation request code to CSSM, CSSM generates an authorization code for the product. After successfully installing the authorization code on the product, the licensing status changes to Registered - Universal License Reservation.

Authorization Status

The different authorization status for Specific License Reservation and Permanent License Reservation in a Unity Connection server are:

- **Evaluation Mode:** Unity Connection remains in Evaluation Mode until the product is not registered with CSSM. In this mode, Unity Connection can use licenses for 90 days.
- **Evaluation Period Expired:** When Unity Connection uses licenses for 90 days without registering with CSSM, the status of Unity Connection changes to Evaluation Period Expired.

- **No License in Use:** When Unity Connection does not use any licenses, the status changes to No License in Use.
- **Authorized - Reserved:** When all the reserved licenses used by Unity Connection are authorized, the status changes to Authorized - Reserved.
- *(Not applicable to Permanent License Reservation)* **Not Authorized - Reserved:** When Unity Connection license usage exceeds the licenses reserved in the virtual account of the product or it uses the feature licenses that are not reserved in the virtual account, the status changes to Not Authorized - Reserved.

Enforcement Policy on Unity Connection

When Unity Connection goes in either of the below state, it will go in enforcement mode. In this mode, user creation or modification in the user account, Speech Connect Port creation or modification and other licensing related updates are not allowed in Unity Connection in enforcement mode. However, existing users can send or receive the voice mails.

- Evaluation Period Expired
- Registration Expired
- Authorization Expired
- Out of Compliance with 90 days of overage period expired.

For more information on the above states, see "Smart Software Licensing Status" section .

Note In case of Specific License Reservation, when Unity Connection goes in either of the below state, it will go in enforcement mode.

- Evaluation Period Expired
- Not Authorized - Reserved state with 90 days of overage period expired

For more information on the above states, see" License Reservation Status, on page 94

In Evaluation Period Expired and Registration Expired states, Unity Connection generates an alarm to disable the encryption on the product. It is recommended that either you execute the "utils cuc encryption disable" CLI command to disable the encryption or register the product with CSSM or satellite to further use the security modules of the Unity Connection.

For more information on the CLI command, see the Command Line Interface Reference Guide for Cisco Unified Solutions for the latest release, available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

For more information on the generated alarm, see Alarm Message Definitions for Cisco Unity Connection available at, https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-system-message-guides-list.html.

Licenses in Unity Connection Cluster

In a Unity Connection cluster, both publisher and subscriber server use licenses but only publisher server is allowed to communicate with CSSM or satellite. Whenever the publisher server communicates with CSSM or satellite, the licensing status and usage information are updated on both publisher as well as subscriber server. In case, when publisher server stops functioning (for example, when it is shut down for maintenance), the subscriber server can use licenses but the licensing status remains unchanged. If the publisher server fails to resume its functioning within 90 days, the user account provisioning is not allowed on subscriber server.

In case of a cluster, only publisher server is allowed to perform the following operations:

- Registration
- Renew Authorization
- Renew Registration
- Deregister
- Reregister

After successful registration of the publisher server with CSSM or satellite, subscriber server only shows the licensing status and usage details of the product.

Migrating Licenses

Whenever you upgrade Cisco Unity Connection from any earlier releases to 14 and later, all licenses (legacy and PLM-based) must be migrated to Cisco Smart Software Licensing. Customers with an active Cisco Software Support Service contract, can convert PLM-based (pre-12.0 versions) licenses to Cisco Smart Software Licenses through the Cisco Smart Software Manager portal at https://software.cisco.com/#SmartLicensing-LicenseConversion via License Registration Portal (LRP) at https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Home. Customers can migrate fulfilled, partially fulfilled, and unfulfilled PAK's or device-based licenses to Cisco Smart Software licenses. For legacy (pre-9.0 versions) licenses, customers must send a license migration request to Cisco Licensing Support available at https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/html/contact.html. For customers with no service contract in place, upgrade SKU's must be ordered which will fulfill the new Cisco Smart Software licenses to their organization's Cisco Smart Account and respective virtual account. Refer the Cisco Collaboration Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html .

For more information on Cisco Smart Software Licensing, please visit http://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.

If HTTPS or Legacy networking is deployed in the system, you can migrate the licenses of each node gradually. It will not affect the system functionality.

Note After upgrading the Unity Connection from any earlier releases to 14, you must register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Enabling Encryption in Cisco Unity Connection

The Category C customers of Unity Connection can enable the encryption on the restricted version of Cisco Unity Connection with both type of licensing – Cisco Smart Software Licensing and Specific License Reservation. To enable the encryption for export restricted virtual account, you must have **CUC Export**

Restricted Authorization Key (PID: CUC-SL-EXRTKY-K9=) license in the virtual account. In addition, you must perform below configuration to enable the encryption for Category C customers.

Caution The **CUC Export Restricted Authorization Key (CUC-SL-EXRTKY-K9=) license is now End-of-Sale (EOS)**.

End-of-Sale Date: August 2, 2020.

End-of-Support Date: August 31, 2025.

This license is no longer available for new purchases. If encryption is required for export-restricted virtual accounts:

1. Customers with existing licenses can continue using them until the End-of-Support date.
2. For new installations or upgrades to Cisco Unity Connection 14 or later, this license is no longer supported.
3. Contact your Cisco representative or reseller to explore alternative licensing options.

Enabling Encryption with Cisco Smart Software Licensing

Do the following procedure to enable the encryption with Cisco Smart Licensing

- Register the Unity Connection with CSSM using token created from Category C customer's virtual account.

Note Unity Connection does not support Cisco Smart Software satellite as deployment option for export restricted virtual account.

- Execute Export request CLI **license smart export request local CUC_Export_Restricted_Authorization_Key** on the registered Unity Connection server to install Export Restricted Authorization Key.
- Execute **utils cuc encryption enable** CLI to enable the encryption on the product and restart the required services mentioned in the CLI output.

You can also perform additional operations by executing the given below CLI commands:

- **license smart export return local CUC_Export_Restricted_Authorization_Key** to return an export restricted feature licenses.
- **license smart export cancel** to cancel the automatic retry of previously failed export request or return from CSSM

For more information on CLI commands, see the applicable version of *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Enabling Encryption with Specific License Reservation

To enable the encryption with Specific License Reservation, you must reserve the **CUC Export Restricted Authorization Key** license in virtual account of Category C customer on CSSM.

For more information on Export Control Functionality, see "Cisco Unity Connection- Restricted and Unrestricted Version" chapter of *Security Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.

License Parameters for Unity Connection Features

Below table describes the Licence Parameters of Unity Connection feature applicable for Cisco Smart Software Licensing and Specific License Reservation.

Table 10: License Parameters for Unity Connection Features

License Parameter	Feature	Description
CUC_BasicMessaging	Total number of voicemail users.	Specifies the maximum number of voice mail users configured in Unity Connection.
CUC_EnhancedMessaging	Total number of enhanced messaging users.	Specifies the maximum number of Unity Connection SRSV users configured on Unity Connection. The Unity Connection SRSV users are reflected under this tag only when the branch is active. This tag also provides the licenses of Basic Messaging.
CUC_SpeechView *(Not applicable for Specific License Reservation)*	Total number of speech view standard users.	Specifies the maximum number of Speech view Standard users configured in Unity Connection.
CUC_SpeechViewPro *(Not applicable for Specific License Reservation)*[1]	Total number of speech view professional users.	Specifies the maximum number of Speech view Professional users configured in Unity Connection.
CUC_SpeechConnectPort	Total number of speech connect ports.	Specifies the maximum number of simultaneous voice recognition sessions and Text to Speech (TTS) sessions allowed in Unity Connection.
CUC_SpeechConnectGuestUser[2]	Total number of Contacts.	Specifes the maximum number of local contacts, along with VPIM contacts created from Non Unity Connection Server.

[1] SpeechViewPro has already been announced EOL. For more information, see https://www.cisco.com/c/en/us/products/collateral/unified-communications/unity-connection/speechview-professional-eol.html.

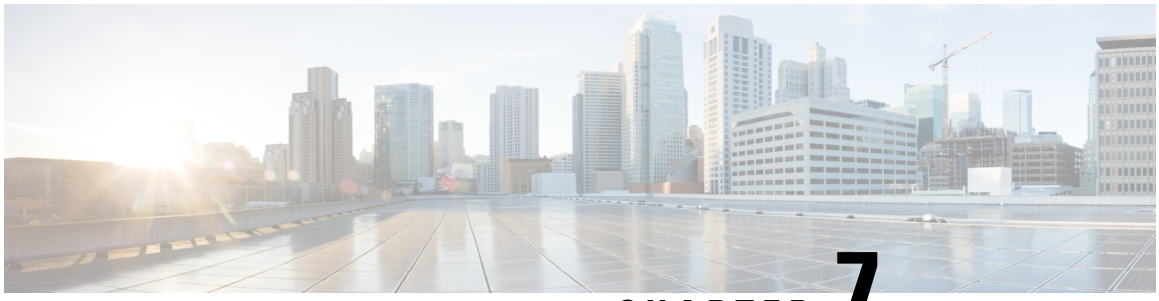
[2] To avail this functionality, customers are currently not required to acquire the Speech Connect Guest User licenses.

Cisco Smart Software Licensing supports license hierarchy, in which higher level licenses are utilized to fulfill the request for lower level licenses to avoid a shortage of the licenses.

Note Reserving entitlement tags of higher release on 12.x is not allowed. You can only borrow higher level licenses on 12.x at CSSM as per license hierarchy.

Following are the licenses included in license hierarchy in an order from higher level to lower level

- Unity Connection Enhanced Messaging User Licenses (12.x)
- Unity Connection Basic Messaging User Licenses (12.x)



CHAPTER 7

Managing Cisco Unity Connection using Cisco Prime Collaboration

Cisco Unity Connection supports Cisco Prime Collaboration Deployment for installation, L2 upgrade and maintenance of Unity Connection.

For detailed information on Cisco Prime Collaboration Deployment, see http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

- Managing Cisco Unity Connection using Cisco Prime Collaboration, on page 101

Managing Cisco Unity Connection using Cisco Prime Collaboration

Cisco Unity Connection supports Cisco Prime Collaboration Deployment for installation, L2 upgrade and maintenance of Unity Connection.

For detailed information on Cisco Prime Collaboration Deployment, see http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Managing Cisco Unity Connection using Cisco Prime Collaboration

INDEX

A

alerts, setting up notification of server status changes 61

C

calls in progress, effects of changing server status 69
changing 62
  cluster settings 62
cluster 72
  how one works 72
Cluster Configuration page, changing settings 62
Connection Server Role Manager service, about 73
critical service, effects of stopping 70
customizing cluster settings 62

D

database replication 72

E

effects 69–70, 73
  of a split-brain condition 73
  of stopping a critical service 70
  on calls in progress when server status changes 69

L

languages 84
  adding to a Connection server (no cluster) (task list) 84

M

message store replication 72
monitoring server status 73

N

notification of server status change alerts, setting up 61

P

ports 63
  assignments of voice messaging to each server 63

R

replication 72
  of database and message store 72
  of voice messages 72

S

server status changes, setting up notification of 61
servers 63, 65, 69, 71, 73
  assignments of voice messaging ports 63
  effects on calls in progress when status changes 69
  shutting down 71
  status functions in cluster 65
  status monitoring 73
setting up notification of server status change alerts 61
settings, customizing cluster 62
shutting down servers 71
split-brain condition, effects of 73
status 65, 73
  of servers 73
  server, functions in cluster 65
stopping a critical service, effects of 70

T

task lists 84
  for adding languages to a Connection server (no cluster) 84

V

voice message replication 72
voice messaging ports, assignments to each server 63