# Installing Cisco Unity Connection



## 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 CDROM drive. 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 15 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 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 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. 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/15/requirements/b_15cucsysreqs.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.
- Unity Connection 15 requires a minimum ESXi version of 7.0 U3 or 8.0 U1 with a minimum VM Hardware version of 17.
- 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.

Prior to the installation, export data from the publisher and subscriber server .

**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 15 available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/networking/guide/b_15cucnetx.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 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/unified_messaging/guide/b_15cucumgx.html

**Exporting data from the publisher and subscriber nodes in the cluster .**

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

Following are the ways to perform Export of data:

- Install the COP file **ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512** on both nodes of cluster.
- Install the COP file **ciscocm.cuc_DataExport_v1.1.k4.cop.sha512** on both nodes of cluster.
- You can use the following 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.

**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 will continue to run in background in case of any network disconnect.

**Different ways supported to perform Install with Data Import:**

1. Once the data is exported from publisher node, import data on destination publisher node and fresh install destination subscriber node.
   a. With above way of data import, in case of Simple Migration , perform the following steps:
      1. Fresh Install Publisher node with Data import .
      2. Fresh Install Subscriber node directly to the above publisher with data import .

**Note** Import data on new virtual machines, using Import option available in Installation wizard. For more information see Installing the Publisher Server, on page 13 section.

**Caution**

1. In case of a cluster network, modifications on cluster page settings on the publisher server is not required.
2. Security password must be the same as from the previous publisher server .

   b. With the above way of data import, incase of Network Migration , perform the following steps:
      1. Fresh Install Publisher node with Data import .
      2. In case of a cluster defined by IP address or hostname on publisher server:
         - Expand System Settings, and select Cluster .
         - Edit and update the Subscriber IP address or hostname .

- Select save.

**Note** Import data on new virtual machines, using Import option available in Installation wizard. For more information see Installing the Publisher Server, on page 13 section.

**Caution**

1. It is adviced to fresh install subscriber node directly to the publisher . Do not delete the old subscriber entry from publisher or reboot the publisher .
2. Security password must be the same as from the previous publisher server .

**Note**

1. Make sure to install **ciscocm.cuc_preUpgradeCheck-005.cop.sha512** 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 15 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: Pre-Installation Tasks 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 ht[illegible] |
| 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. |

| | Task | Important Notes |
|---|---|---|
| Step 4 | Configure an external NTP server during a Unity Connection server installation.<br><br>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.<br><br>To verify the NTP status of the publisher server, log into the Command Line Interface on the publisher server and enter the following command:<br><br>**utils ntp status** | For more information, see the Command Line Reference Guide for Cisco Unified Solutions fo release, available at http://www.cisco.com/en/us/products/unified-communications/unity-connection/products-mainte<br><br>**Caution** If the publisher server fails to syn with an NTP server, installation o subscriber server can also fail. |
| 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 co Cisco servers. With PortFast enabled, the swi immediately brings a port from the blocking s the forwarding state by eliminating the forwar [the amount of time that a port waits before cl from its Spanning-Tree Protocol (STP) learni 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 the 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:<br><br>https://software.cisco.com/download/navigator.html?mdfid=280 |

# 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.

**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.

**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 the 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

**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

**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 2: Gathering Information for Installation 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).<br>Select the time zone that most closely matches the location of your server.<br>**Caution** In a cluster, you must set the subscriber server to the same time zone as the publisher server. | Yes, using the CLI command<br>CLI > **set timezone** |
| **MTU Size: _____** | Sets the largest packet, in bytes, that is transmitted by this host on the network.<br>By default, MTU is set to the size defined in the operating system.<br>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.<br>The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network.<br>**Note** In clustered server pairs, the MTU setting must be the same on both servers | Yes, using the CLI command<br>CLI > **set network mtu** |

| Configuration Setting | Description | Can Setting Be Changed After I |
|---|---|---|
| **Hostname and IP addresses:**<br>DHCP (Yes/No): _____<br>If DHCP is **No**:<br>Hostname: _____<br>IP Address: _____<br>IP Mask: _____<br>Gateway (GW) Address:_____ | Sets whether to use DHCP to automatically configure the network settings on your server.<br>If you select **No**, you must enter a hostname, IP address, IP address mask, and the gateway IP address.<br>The hostname can contain up to 50 alphanumeric characters, hyphens, underscores, and period. The first character cannot be a hyphen.<br>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<br>**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.<br>**Caution** Make sure not to use ciscounity in the hostname of the server else enterprise replication gets broken. | Yes, using the CLI command<br>CLI > **set network dhcp**<br>CLI > **set network gateway**<br>CLI > **set network ip eth0** |
| **Domain Name Server:**<br>DNS: (Yes/No): _____<br>If DNS is **Yes**:<br>Domain: _____<br>DNS Primary: _____<br>DNS Secondary: _____ | Sets whether a DNS server resolves a hostname and IP address.<br>**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<br>CLI > **set network dns**<br>CLI > **set network domain** |

| Configuration Setting | Description | Can Setting Be Changed After Inst |
|---|---|---|
| **Administrator Account Credentials:**<br>Login: _____<br>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.<br>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.<br>**Note** Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore. | Login: No.<br>Password: yes, using the CLI comm<br>CLI > **set password user admin**<br>**Note** You can create additio administrator accounts installation. |
| Certificate Information:<br>Organization: _____<br>Unit: _____<br>Location: _____<br>State: _____<br>Country: _____ | Sets information used by the server to generate certificate signing requests (CSRs) that are used to obtain third-party certificates.<br>**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.<br>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<br>CLI > **set web-security** |
| **Cluster:**<br>First server in cluster (Yes/No): ____<br>If First server is **No**:<br>Publisher hostname: _____<br>Publisher IP address: _____<br>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:**<br>NTP Server 1: _____<br>NTP Server 2: _____<br>NTP Server 3: _____<br>NTP Server 4: _____<br>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.<br>The NTP service ensures that the time synchronized is accurate for date/timestamps of messages, reports, and various tools, such as logs and traces.<br>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.<br>**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.<br>The NTP server that you specify for the publisher server is automatically applied for the subscriber server. | Yes, using Cisco Unified Opera Administration:<br>**Settings > NTP Servers**<br>Using the CLI command<br>CLI > using the CLI command |
| **Security Password** | Sets the password used by a subscriber server to communicate with a publisher server.<br>The security password is also used by the Disaster Recovery System to encrypt backups.<br>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<br>CLI > **set password user secu**<br>**Caution** If you are changing password in a clus pair you must char security password servers and reboot For more informat description of this the Command Lin Reference Guide f 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.<br>The hostname can contain alphanumeric characters, hyphens, or periods but it must start with an alphanumeric character.<br>**Note** You must specify an SMTP server if you plan to use electronic notification. | Yes, using the CLI command:<br>CLI > **set smtp** |
| **Application Account Credentials:**<br>Login: _____<br>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<br>CLI > **utils cuc reset password** |

# Installation Scenarios

*Table 3: Installation Scenarios*

| Installation Scenarios | Installation Method |
|---|---|
| Standalone Deployment | Standard<br>• Installing the Publisher Server<br>• Verifying the Installation<br>Unattended<br>• Generating Answer File for Unattended Installation<br>• Installing the Publisher Server<br>• Verifying the Installation |

| Installation Scenarios | Installation Method |
|---|---|
| Cluster Deployment | Standard<br>• Installing the Publisher Server<br>• Configuring Subscriber Server on the Publisher Server<br>• Installing the Subscriber Server<br>• Verifying the Installation<br>Unattended<br>• Generating Answer File for Unattended Installation<br>• Installing the Publisher Server<br>• Configuring Subscriber Server on the Publisher Server<br>• Installing the Subscriber Server<br>• 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 4: Installation Wizard Navigation.

***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.

**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.
- 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 CDROM drive 2. Create the config files with .iso extension and attach the .iso to this drive 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

**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 15 release.
- If **Import** option is not selected, while installation for Unity Connection 15 release.
- If **Import** option is selected only for publisher node, while installing Unity Connection 15 release.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.

**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 28. 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 CDROM drive, 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 CDROM drive 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,attach the .iso to this drive.
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 the Publisher Server and Installing the Subscriber Server section.

### Generating and Downloading Answer File

**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

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

**Step 2** Select the CDROM drive 1 and 2 > Connect to ISO image on local disk option from the toolbar and select CDROM drive 1 and 2 > 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 3** (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

**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 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 the config files with .iso extension and attach the .iso to CDROM drive 2.
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 server, see the Installing the 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/en/US/products/ps6509/prod_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/en/US/products/ps6509/prod_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.

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.

**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.

**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.

**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.

**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.

**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 Upgrading from a Local Disk.

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 Upgrading from a Local Disk 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.

**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 15 at* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/serv_administration/guide/b_15cucservag.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.
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 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucm_sip/b_15cucintcucmsip.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 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucm_sip/b_15cucintcucmsip.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/15/quick_start/guide/b_15ucqssamlsso/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.

### 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.

# 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.

For more information on troubleshooting installation issues, see the *Troubleshooting Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/troubleshooting/guide/b_15cuctsg.html.