Cisco Prime Collaboration Deployment Features

- Cisco Prime Collaboration Deployment Considerations, on page 1
- Network Address Translation Support, on page 3
- Supported Tasks for Applications and Versions, on page 4
- Upgrade Paths for Export Restricted and Unrestricted Software, on page 9
- Supported ESXi Server Versions, on page 10
- Cluster Inventory, on page 10
- Task Management, on page 17
- Administration Tools, on page 50
- FIPS 140-2 Compliance, on page 62
- EnhancedSecurityMode Support, on page 62
- Re-encryption through AES, on page 64
- Limited Number of Sign-in Sessions, on page 64
- Minimum TLS Version Control, on page 65
- Configurable Maximum Install Timeout for Clusters, on page 65

Cisco Prime Collaboration Deployment Considerations

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

Step	Tasks
Step 1: Inventory Creation	To perform any tasks, you must first have clusters in your inventory. To add a UC cluster that is already running UC applications to your inventory, click **Open and close navigation** and choose **Inventory** > **Clusters** > **Discovery Cluster** feature. To migrate an existing cluster to new virtual machines, click **Open and close navigation** and choose **Inventory** > **Clusters** > **Define Migration Destination Cluster**. (See Migration Task, on page 18.) To install a new cluster, click **Open and close navigation** and choose **Inventory** > **Clusters** > **Define New UC Cluster** feature. (See Install Task, on page 42.) If you are migrating an existing cluster to a new virtual machine cluster, or installing a new cluster, you must first add the ESXi Hosts that contain those virtual machines to your inventory. To add an ESXi host, click **Open and close navigation** and choose **Inventory** > **ESXi Hosts**. (See Add an ESXi Host Server, on page 13.)
Step 2: Create a Task	You can create a task to perform an operation on a cluster in your inventory. During task creation, options allow you to: • Choose the cluster **Note** This task depends on the type of cluster you require. For example, you may choose a discovered cluster or a migration cluster. • Determine when to run the task • Determine if the task should run independently or pause between steps To perform one of the following actions, select from these procedures: • To migrate from an existing cluster to a new cluster of VM machines, see Migration Task, on page 18. • To upgrade the Unified Communications Manager version of an existing cluster, see Upgrade Task, on page 31. • To switch the version of an existing cluster, see Switch Versions Task, on page 36. • To restart an existing cluster, see Server Restart Task, on page 38. • To change the hostname or IP address of one or more servers in an existing cluster, see Readdress Task, on page 40. • To create a new UC cluster from VM machines, see Install Task, on page 42.
Step 3: Monitor Tasks	After a task is created, you can use the Monitoring window to view or track any task. You can also use this page to cancel, pause, or resume tasks. To view the tasks you created, see Monitor Task Status, on page 49.
Step 4: Administrative Tasks	You can set up email notification. See Email Notification.

Network Address Translation Support

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

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

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

Configure Cisco Prime Collaboration Deployment Behind the NAT

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

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

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

Procedure

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

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

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

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

Supported Tasks for Applications and Versions

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

- Table 1: Supported Tasks for Cisco Unified Communications Manager (including Session Management Edition), on page 5
- Table 2: Supported Tasks for Cisco Unified Presence, on page 6
- Table 3: Supported Tasks for the IM and Presence Service, on page 7
- Table 4: Supported Tasks for Cisco Unified Contact Center Express, on page 8
- Table 5: Supported Tasks for Cisco Unity Connection, on page 8

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

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

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

Note If you are using Cisco Prime Collaboration Deployment to migrate Cisco Unified Communications Manager from Release 12.0(1) to any higher release, you must install the following COP file on your 12.0(1) system before you begin the migration. Otherwise, the configuration files that are related to Smart Licensing will not be migrated.

```
ciscocm-slm-migration.k3.cop.sgn
```

This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Cisco Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Cisco Unified Communications Manager 12.0(1)SU1, you don't need to install the COP file.

Warning With this release, network migration from MCS to the virtual machine scheduled for Cisco Unified Communications Manager and IM and Presence 12.0(1) using Prime Collaboration Deployment 12.0(1a) causes IM and Presence installation issues due to Cisco Unified Communications Manager's open defect.

Perform the following workaround before installing IMP with the help of TAC:

1. Replace old IM and Presence pub IP address entry with new IP address in processnode.xml file of Cisco Unified Communications Manager
2. Add new IM and Presence pub entry on **System** > **Server list** on Cisco Unified Communications Manager
3. Retry IM and Presence pub installation from Cisco Prime Collaboration Deployment

Note Check destination application version release notes for any known caveats with using the Cisco Prime Collaboration Deployment tasks with the application. For Cisco Prime Collaboration Deployment, Fresh Install, Migrate and Upgrade tasks, check the destination application's Installation Guide and Upgrade Guide for any application-specific rules or restrictions on using these Cisco Prime Collaboration Deployment tasks with the application (e.g. required node sequencing for installs or upgrades, restrictions on how COPs may be installed, etc.).

Table 1: Supported Tasks for Cisco Unified Communications Manager (including Session Management Edition)

Task	Release
Cluster Discovery	6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1)
Migrate Cluster (Install Application and Import Data from Old System)	**From** 6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1) **To** 10.x, 11.x, or 12.0(1) **Note** Prime Collaboration Deployment Migration 11x (till 11.5 SU5)/12.0 to 11x (till 11.5 SU5)/12.0 isn't supported, if "11x (till 11.5 SU5)/12.0" is an identical version as in same major, same minor, same MR, same SU/ES between the source and destination.

Task	Release
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1) **To** 10.x, 11.x, or 12.0(1)
Restart	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1),12.0(1)
Switch Version	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.x, 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1)
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.x, 11.0(1), 11.5(1), 12.0(1)

Note When you perform any task (Cluster Discovery, Migrate Cluster, Upgrade Cluster, Restart, Switch Version) in 6.x or 8.x (configured FIPS mode) version, you cannot perform a simultaneous task as there is a change in the cipher version. If you try to perform any simultaneous task, then it fails.

Table 2: Supported Tasks for Cisco Unified Presence

Task	Release
Cluster Discovery	8.5(x), 8.6(x)
Migrate Cluster (Install Application and Import Data from Old System)	**From** 8.5(4), 8.6(3), 8.6(4), 8.6(5) **To** 10.x, 11.x, or 12.0(1)
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 8.6(3), 8.6(4), 8.6(5) **To** 10.x, 11.x, or 12.0(1)
Restart	8.6(3), 8.6(4), 8.6(5)
Switch Version	8.6(3), 8.6(4), 8.6(5)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	Not applicable

Task	Release
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	Not applicable

Table 3: Supported Tasks for the IM and Presence Service

Task	Release
Cluster Discovery	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1), 12.0(1)
Migrate Cluster (Install Application and Import Data from Old System)	**From** 9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1) **To** 10.x, 11.x, or 12.0(1) **Note** Network migrations from MCS to Virtual Machine scheduled for 12.0(1) is not supported. **Note** Prime Collaboration Deployment Migration 11x (till 11.5 SU5)/12.0 to 11x (till 11.5 SU5)/12.0 isn't supported, if "11x (till 11.5 SU5)/12.0" is an identical version as in same major, same minor, same MR, same SU/ES between the source and destination.
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**From** 9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1), 12.0(1) **To** 10.x, 11.x, or 12.0(1)
Restart	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1), 12.0(1)
Switch Version	9.0(1), 9.1(1), 10.x, 11.0(1), 11.5(1), 12.0(1)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.x, 10.5(1), 10.5(2), 11.0(1), 11.5(1), 12.0(1)
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	Not Supported

Table 4: Supported Tasks for Cisco Unified Contact Center Express

Task	Release
Cluster Discovery	8.5(1), 9.0, 9.0(2), and 10.x, 11.x 12.x
Migrate Cluster (Install Application and Import Data from Old System)	Not Supported
Upgrade Cluster (Upgrade Application Version or Install COP Files)	**Release Supported:** • **From** 10.5(x), 10.6(x), 11.x **To** 12.0 • **From** 11.6(x), 12.0 **To** 12.5
Restart	9.0(2), 10.x, 11.x 12.x
Switch Version	9.0(2), 10.x, 11.x 12.x
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.5(x), 11.x 12.x
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.5(x), 11.x 12.x

Note : When you perform any task (Upgrade Cluster, Fresh Install New Cluster, or Edit or Expand an Existing Cluster) from Unified Contact Center Express, you cannot use the touchless installation method. The user needs to enter the details manually. For more information on the installation process, see the *Installation Guide and Upgrade Guide* of Cisco Unified Contact Center Express

Table 5: Supported Tasks for Cisco Unity Connection

Task	Release
Cluster Discovery	8.6(1), 8.6(2), 9.x, 10.x, 11.0(1), 11.5(x),12.0(1)
Migrate Cluster (Install Application and Import Data from Old System)	Not Supported
Upgrade Cluster (Upgrade Application Version or Install COP Files)	From 8.x, 9.x, 10.x, 11.0, 11.5, 12.0(1) To 10.x, 11.x, 12.0(1)

Task	Release
Restart	8.6(1), 8.6(2), 9.x, 10.x, 11.0(1), 11.5(x), 12.0(1)
Switch Version	8.6(1), 8.6(2), 9.x, 10.x, 11.0(1), 11.5(x), 12.0(1)
Fresh Install New Cluster or Edit or Expand an Existing Cluster	10.5(x), 11.0(1), 11.5(x), 12.0(1)
Readdress (Change Hostname or IP Addresses for One or More Nodes in a Cluster)	10.5(x), 11.0(1), 11.5(x), 12.0(1)

Related Topics

Create an Upgrade Task, on page 31
Create a Switch Versions Task, on page 36

Upgrade Paths for Export Restricted and Unrestricted Software

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

Table 6: Supported Upgrade Paths for Export Restricted and Unrestricted Software

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

Related Topics

Create an Upgrade Task, on page 31
Create a Switch Versions Task, on page 36

Supported ESXi Server Versions

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

VMware vSphere ESXi on Host having VM of Cisco Unified Communications Manager or Another Application	Cisco Prime Collaboration Deployment Version Compatibility for VMware APIs
5.1 and older	No
5.5	No
6.x	• No—For Release 11.5(1) • Yes—For Release 11.5(1) SU1 and later
7.0	Yes—For Release 12.6 and later

Cluster Inventory

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

Discover a Cluster

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

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

From 10.x and above UC clusters, Cisco Prime Collaboration Deployment uses SOAP requests to pull platformConfig.xml file from UC nodes. The cop file “ciscocm.ucmap_platformconfig.cop” is installed if Platform Administrative Web Service(PAWS) is not available.

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

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

If you are upgrading IM and Presence Services nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading Cisco Unified Communications Manager nodes, following rules apply:

- If you are using the Unified CM OS Admin interface for upgrade, you must upgrade the Cisco Unified Communications Manager publisher node and then upgrade the IM and Presence Services nodes to an MR or an ES Release.
- If you are using the Cisco Prime Collaboration Deployment migration task, choose the Cisco Unified Communications Manager publisher node in addition to the IM and Presence Services nodes.
- If you are using the Cisco Prime Collaboration Deployment upgrade task, you do not need to select the Cisco Unified Communications Manager publisher node if the first three digits of new version of IM and Presence Services match the first three digits of the currently installed version of Cisco Unified Communications Manager.

Procedure

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

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

Step 3 Enter details in the following fields:

- **Choose a Nickname for this Cluster**
- **Hostname/IP Address of Cluster Publisher**

  Note For a cluster that has both Unified Communications Manager and IM and Presence Service nodes, enter the hostname or IP address of the Cisco Unified Communications Manager publisher.

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

- **OS Admin Username**
- **OS Admin Password**

  Note Ensure that cluster password is less than 16 characters.

- **Enable NAT**

Step 4 (Optional) Check the **Enable NAT** check box, and then click **Next**.

Important During discovery, the `ciscocm.ucmap_platformconfig.cop` file is installed automatically on the active partition of all nodes in the cluster. This COP file is used for the cluster discovery process and does not affect Cisco Unified Communications Manager.

Note When a cluster is behind NAT, the application tries to establish communication with each node using its private address. So, the nodes are unreachable. A pop-up shows the unreachable nodes.

Cisco Prime Collaboration Deployment generates a list of cluster nodes from the inventory of the publisher server. The list generation process may take several minutes to complete. After the list is generated, a confirmation message appears to indicate the completion of the cluster discovery process.

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

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

Step 7 Click **Next**.

Step 8 (Optional) Click **Assign Functions** to assign functions to each of the cluster nodes.

Note The assignment of functions has no effect on the services that are to be activated. However, this information can be used to determine the default sequence of tasks.

The **Assign Functions** dialog box appears.

Step 9 Click **Finish**.
The cluster appears in the **Clusters** window, showing the cluster name, the product and version, the cluster type as `Discovered`, and the discovery status.

Note It might take a few minutes to discover a cluster. After the discovery is complete, the information for each node in the cluster is listed in the **Cluster Inventory** window. If you cancel the discovery before it is complete, the data is lost and you will have to repeat the discovery procedure.

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

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

Related Topics

Supported Tasks for Applications and Versions, on page 4
Upgrade Paths for Export Restricted and Unrestricted Software, on page 9

Modify and View a Cluster

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

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

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

Procedure

Step 1 Discover a cluster by following the Discover a Cluster procedure. See Discover a Cluster, on page 10.

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

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

Step 4 Click **OK**.

Add an ESXi Host Server

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

To communicate with an ESXi host server, Cisco Prime Collaboration Deployment requires either root access to the ESXi software or a nonroot user with **Host(Configuration, Storage Partition Configuration)** and **Virtual Machine(Interaction, Configure CD Media, Configure Floppy Media, Device Connection, Power Off, and Power On)** privileges enabled. The administrator creates a nonroot user with the specific permissions for Cisco Prime Collaboration Deployment tasks, such as Interactions, Configure CD Media, Configure Floppy Media, Device Connection, Power Off, and Power On privileges, for the fresh install or migration. The length of the nonroot user password must be less than 16 characters.

For more information on user password, see the Frequently Asked Questions About the Installation.

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

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

Note Ensure that the ESXi password is less than 32 characters, cluster password (install/discovered/migration) is less than 16 characters and are compliant with the preceding section that describes allowable special characters.

Procedure

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

Step 2 Click **Add ESXi Host**.

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

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

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

Create a Migration Cluster

Before you begin

To create a migration task, perform the following procedure:

1. Discover the existing cluster that you wish to migrate. See the "Discover a Cluster" procedure at Discover a Cluster, on page 10.
2. Define a migration cluster.

Note After you define the migration cluster, see "Migration Task" at Migration Task, on page 18 to define when and how to perform the migration.

Procedure

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

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

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

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

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

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

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

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

The **Configure Destination Cluster** window appears.

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

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

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

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

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

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

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

Important You cannot change the domain name during a migration.

Step 11 Click **Finish**.

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

Add New Cluster for Fresh Install

Procedure

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

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

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

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

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

a) In Network section, select either **Static IP Address** or **Use DHCP with reservations**. If you select the **Static IP Address** option, enter the hostname, IP Address, subnet mask, gateway, and NAT IP. If you select **Use DHCP with reservations** option, enter the IP address that you have a reservation for on your DHCP server (associated with the MAC address for that VM) in addition to the hostname.

If you are adding a Cisco Unified Contact Center Express server, do not use DHCP for network settings.

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

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

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

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

d) Click **OK**.

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

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

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

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

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

Step 9 Enter the OS administration credentials, application credentials, security password, SMTP settings, and certificate information for this cluster, and click **Next**.

Note Before you enable FIPS mode, Common Criteria, or Enhanced Security Mode, ensure that you have minimum 14 characters for Security Password.

The **Configure DNS Settings** window appears.

Step 10 (Optional) Add a DNS setting for a node, select the node, and click **Assign DNS Settings**.

The Cisco Unified Contact Center Express application must use DNS.

The **Configure NTP Settings** window appears.

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

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

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

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

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

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

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

Task Management

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

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

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

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

Note Migration and install .iso files must be bootable.

Note PCD scheduler can execute 21 task actions simultaneously.

Migration Task

Before You Begin

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

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

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

2. **ISO file**—Download the recommended OVA and ISO images for the target release, and use SFTP to send the ISO file to the Cisco Prime Collaboration Deployment server, `/fresh_install` directory.
3. **VMware**—Deploy the Cisco-recommended OVA to create the VMs for the destination nodes. Create the appropriate number of target virtual machines on your ESXi hosts (one new virtual machine for each server in the existing cluster) using the Cisco OVAs that you downloaded in Step 2. Configure the network settings on new VMs.
4. **Cisco Prime Collaboration Deployment GUI**—Add the ESXi Hosts that contain your virtual machines to the Cisco Prime Collaboration Deployment inventory. For information about adding an ESXi host to Cisco Prime Collaboration Deployment, see Add an ESXi Host Server, on page 13.
5. **Cisco Prime Collaboration Deployment GUI**—Ensure that you performed a cluster discovery for the existing cluster (source cluster) so that it appears in the Cluster Inventory. For information about cluster discovery, see Discover a Cluster, on page 10.
6. **Cisco Prime Collaboration Deployment GUI**—Create the migration cluster (click **Open and close navigation** and choose **Inventory** > **Clusters**) to define the mapping between MCS source nodes and target virtual machines.

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

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

7. **Cisco Prime Collaboration Deployment GUI**—Setup Email Notification (Optional)
   - Click open and close navigation and choose **Administration** > **Email Notification**.
   - When email notification is set up, the Prime Collaboration Deployment server emails the error conditions that may occur during the migration task.
8. **Cisco Prime Collaboration Deployment GUI**—Create the migration task.
9. Install the `ciscocm.migrate_export_10_0_1.sh_v1.1.cop.sgn` cop file on both IM and Presence publisher and subscriber nodes.

Special Considerations

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

Note

1. Before migration the cluster, Cisco recommends install the latest Upgrade Readiness COP file. Refer to the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* for details. This is applicable if the source cluster is 9.X or above and valid only for Unified Communications Manager and IM&P.
2. Make sure Prime Collaboration Deployment has enough free space depending on the size of the source cluster in the common partition.

Create a Migration Task

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

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

Procedure

Step 1 Click **Open and close navigation** and choose **Task** > **Migrate**.

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

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

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

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

Important The ISO file is visible here only if it was placed in the local SFTP directory under `/fresh_install`, if Prime Collaboration Deployment is used as local SFTP. If any remote SFTP is associated with the migration cluster, then the files should present in the remote SFTP.

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

Note When you add the Remote SFTP server, you should maintain the different SFTP directories for fresh install/migration and upgrade. You can add the same Remote SFTP server for fresh install/migration and upgrade but directories for fresh install/migration and upgrade should be different.

Step 6 Click **Next**.

Step 7 In the **Specify Migration Procedure** section, you will see the default sequence for the migration task. If you wish, you can change the sequence of steps in the migration procedure. (For example, the default is to install each subscriber individually. You might want to change this to install more than one subscriber in a step.) You have the following options:

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

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

- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.

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

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

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

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

Note Cisco Prime Collaboration Deployment does not allow you to select the date and time for the dependent tasks, as the dependent task starts automatically after the successful completion of the existing task.

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

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

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

  Note If you choose to start the task manually, a task is created, but does not start until you click the **Start task** button on the Monitoring page, or the **Start task** link on the task page.

- Select **Start task immediately upon completion of this wizard** to start the task immediately after you click **Finish**.
- If you want the system to automatically switch to the new version, choose the option **Upgrade Option to Automatically Switch to New Version after Successful Upgrade**.

Step 9 Click **Next**.

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

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

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

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

Related Topics

Supported Tasks for Applications and Versions, on page 4

Upgrade Paths for Export Restricted and Unrestricted Software, on page 9

Run a Migration Task

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

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

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

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

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

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

Unified CM source cluster - from Release	Simple Migration or Network Migration	Unified CM source cluster - (secure or nonsecure)	User procedures to be performed during migration
6.1(5), 7.1(3), 7.1(5)	Simple migration	Secure	No steps are required during migration.
6.1(5), 7.1(3), 7.1(5)	Simple migration	Nonsecure	No steps are required during migration.
6.1(5), 7.1(3), 7.1(5)	Network migration	Secure	When migration task reaches the Forced Pause step, click Resume.
6.1(5), 7.1(3), 7.1(5)	Network migration	Nonsecure	When migration task reaches the Forced Pause step, click Resume.
8.x, 9.x, and 10.x	Simple migration	Secure	No steps required during migration.
8.x, 9.x, and 10.x	Simple migration	Nonsecure	No steps required during migration.

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

Postmigration Tasks for Cisco Unified Communication Manager Nodes in the Cluster

“After the migration task runs successfully, if a migration task with network migration is performed, some additional steps is required. (No postmigration tasks are required if a simple migration is performed.) ”

Consult the following table and the applicable migration Use Case flowchart to determine whether any user tasks should perform after the migration task is successful.

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

Note Device default settings will **NOT** be carried over from source cluster to destination cluster after a simple or network migration task.

Any device packs installed for specific features need to be reinstalled if destination cluster version does not already include the device pack feature.

Note After migration, reinstall all COP files for any country locale that you are using. COP files may be reinstalled through PCD Upgrade Task or Unified Communications Manager OS Admin or CLI.

Post Migration Tasks for IM and Presence Service

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

Procedure

	Command or Action	Purpose
Step 1	Configure certificates and certificate trust stores.	If the old cluster had CA-signed certificates in any of the component trust stores, be aware that the components contain self-signed certificates on the migrated Release 10.x cluster. Also, the root and intermediate certificates of the Certificate Authority are not preserved in their respective trust stores. You should sign the certificates with the old Certificate Authority, similar to how it would have been done initially. For more information, see the *Administration Guide for Cisco Unified Communications Manager Guide*.
Step 2	Configure intercluster peers.	If the old cluster had an intercluster peer relationship, you need to delete the configuration from all peer clusters. Once this is done, add the appropriate interclustering based on the network details of the new cluster. For example, Cluster A, Cluster B, and Cluster C are all intercluster peers. If Cluster A was migrated, then you should delete all interclustering configuration from the old Cluster A and likewise Cluster A from Cluster B and Cluster C and then add interclustering with the network details of the new Cluster A. You do not need to configure anything from the

	Command or Action	Purpose
		new Cluster A since the migration brings over the old data. For more information, see *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager.*
Step 3	Re-publish SIP Federation.	If the old cluster was front-ending SIP Interdomain with Microsoft OCS/Lync/AOL or SIP Intradomain federation with OCS/Lync, then your enterprise needs to re-publish the DNS-SRV of your federating domain to reflect the new network details. If the far side has SIP static routes that are configured instead of DNS-SRV based routing, then the SIP static routes need to be changed to reflect the new network address. Similarly, all intermediate network elements (including ASA or any other similar components that route or inspect traffic to the old cluster from the external federation entities) need to be re-configured for successful routing to the new cluster. For Interdomain configuration, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*. For Intradomain federation, see *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.
Step 4	Re-publish XMPP Federation.	If the old cluster was front-ending XMPP Interdomain federation to any external XMPP servers, then your enterprise needs to republish your federating domain's DNS-SRV records to reflect the new network details. For more information, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.
Step 5	Configure Cisco Jabber/Cisco Unified Personal Communicator connectivity.	Jabber or Unified Personal Communicator caches the hostname information from the old cluster and does not have new hostname information unless you are able to push the configuration to the desktop of the user, or that user manually enters one of the node names. A fail safe approach for users that are unassigned from the old cluster, and as a result are unable to log in, involves the user manually entering the hostname or IP address of one of the nodes in the new cluster (of which they were

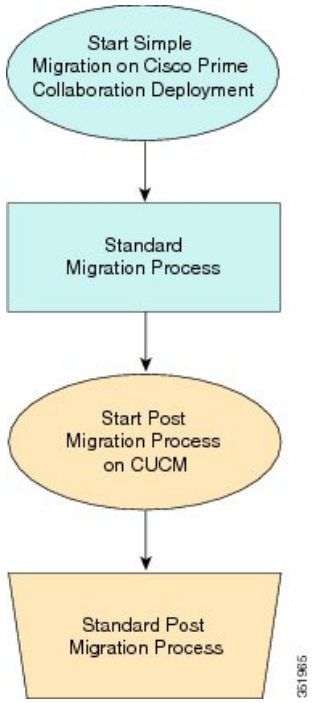
	Command or Action	Purpose
		informed before migration). In this scenario, the user's client finds the right home node by way of redirected login.

Migration Procedure Flow Charts

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

Simple Migration

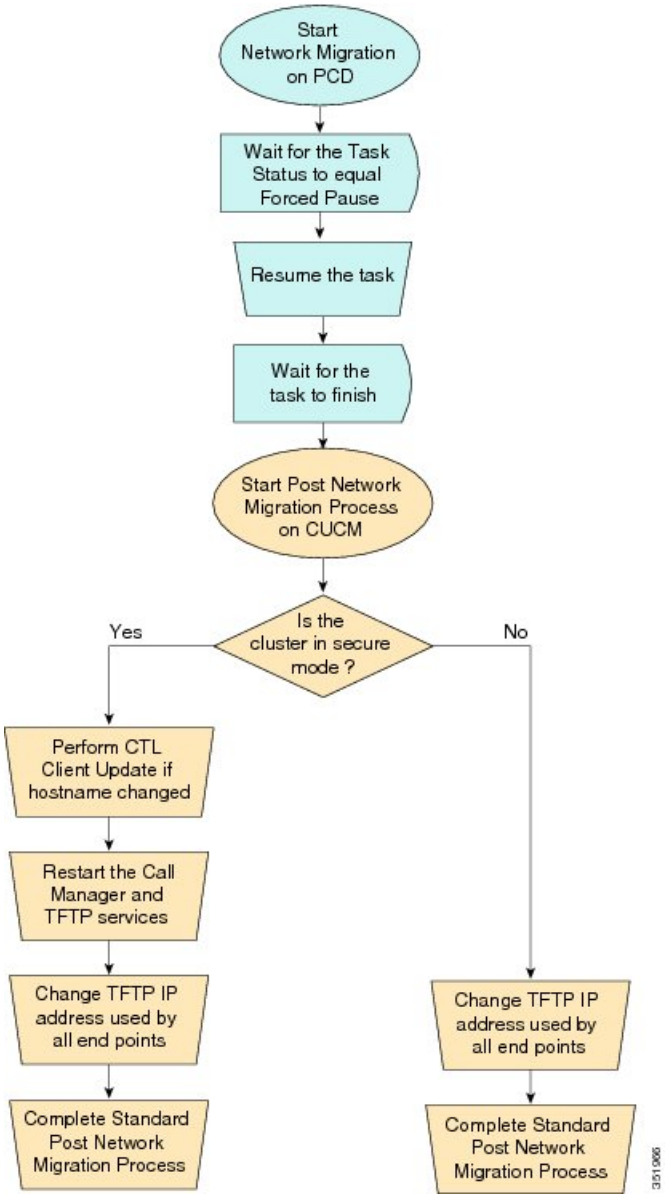
Figure 1: Flow Chart for Simple Migration



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

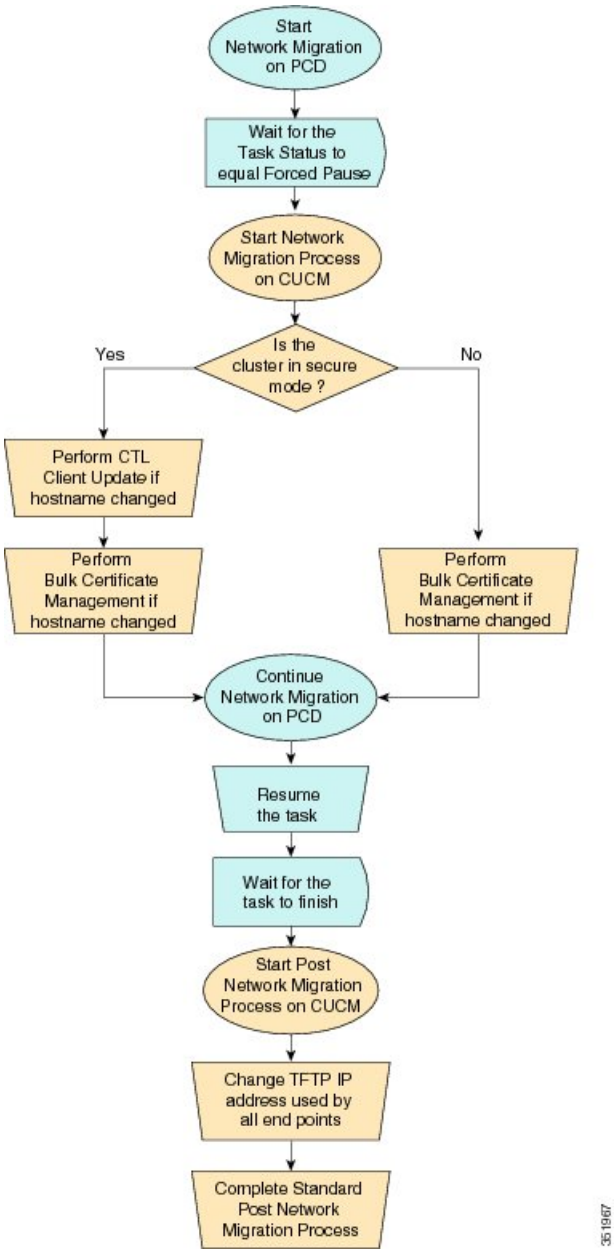
Pre Release 8.0.1 Unified CM Network Migration

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



Release 8.0.1 And Later Unified CM Network Migration

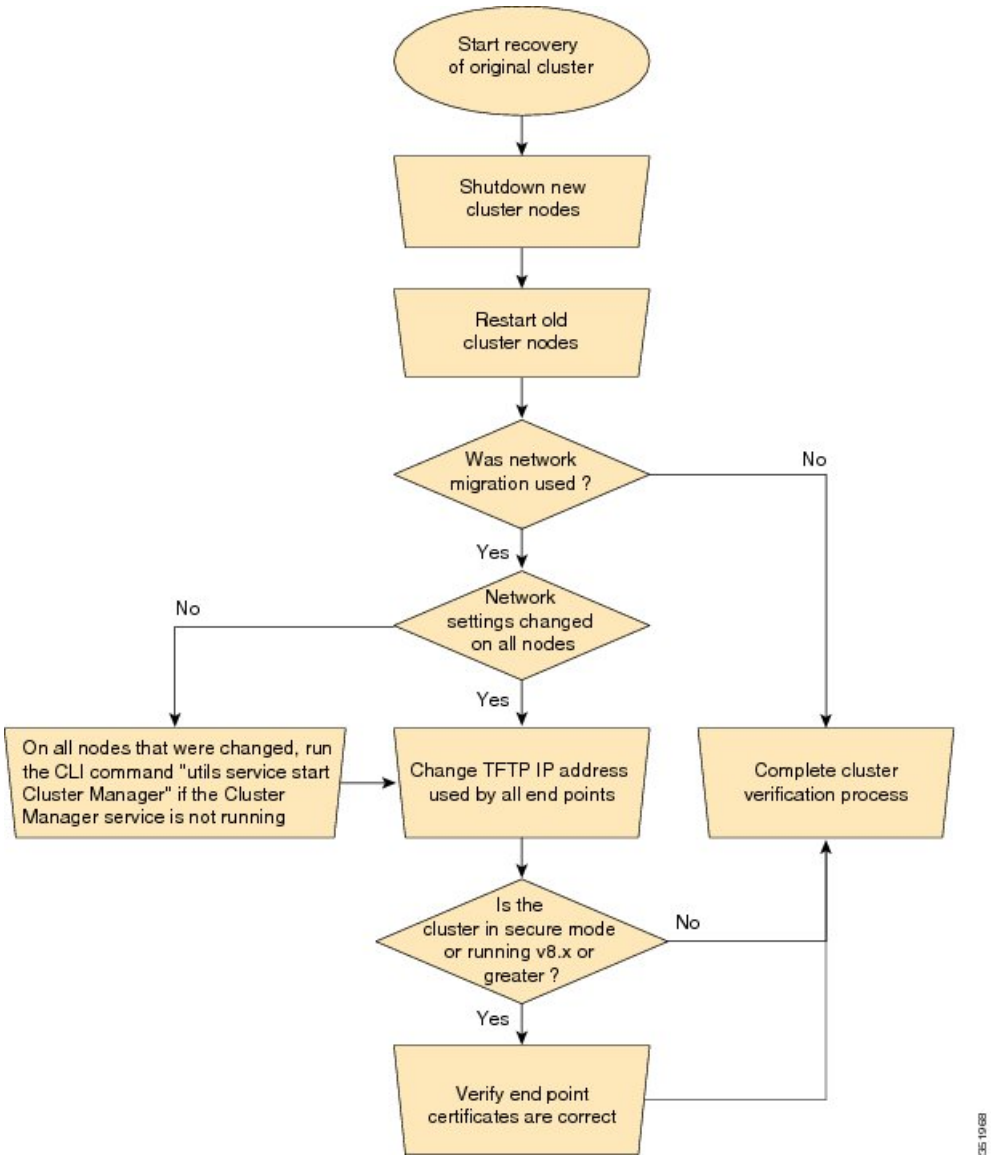
Figure 3: Flow Chart for Release 8.0.1 and later Unified CM Network Migration



Recovery of Original Cluster

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

Figure 4: Flow Chart for Recovery of Original Cluster



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

The steps below are used if a migration task fails when there were network migration changes on one or more nodes. Following the failure, you may need to perform some steps to get the old cluster nodes running again. See the flow chart above for all steps to be followed. Below are detailed steps for running the CLI command to restart cluster manager on old nodes.

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

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

Use Case 1

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

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

Use Case 2

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

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

Use Case 3

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

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

Use Case 4

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

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

Procedure

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

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

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

Upgrade Task

Use Cisco Prime Collaboration Deployment to perform the following types of upgrade tasks:

- Direct standard upgrade—This upgrade does not require upgrades to the embedded operating system. You can install upgrade software on your server while the system continues to operate.
- Direct refresh upgrade—This upgrade is required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the embedded operating system changes between the version you are upgrading from and the version that you are upgrading to.

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

Create an Upgrade Task

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

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

Note Based on the source version and destination version you choose, Cisco Prime Collaboration Deployment uses either direct standard upgrade sequence or validation, or direct refresh upgrade sequence or validation.

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

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

Before you begin

1. Note the supported restricted and unrestricted paths. See “Supported Upgrade and Migration Tasks” and “Upgrade Paths for Export Restricted and Unrestricted Software” in the Related Topics section.
2. Perform a cluster discovery for the cluster that you wish to upgrade, so it appears in the Cluster Inventory. See Discover a Cluster, on page 10.
3. Download the ISO files you wish to upgrade to, and use SFTP to send this file to Cisco Prime Collaboration Deployment in the upgrade folder. If you are using the upgrade task to install a .cop file, upload the .cop file to the /upgrade folder using an SFTP client.
4. For the application servers in the cluster to be upgraded, ensure that the Platform Administrative Web Service is active on that server.

Note Before upgrading the cluster, Cisco recommends to install the latest Upgrade Readiness COP file. Refer to the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* for details. This is applicable if the source cluster is 9.X or above and valid only for Unified Communications Manager and IM&P.

Procedure

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

Step 2 Click **Add Upgrade Task**.

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

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

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

Step 6 Click **Next**.

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

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

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

Step 8 Select a valid upgrade file or files.

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

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

Note When you add the Remote SFTP server, you should maintain the different SFTP directories for fresh install/migration and upgrade. You can add the same Remote SFTP server for fresh install/migration and upgrade but directories for fresh install/migration and upgrade should be different.

Step 9 Click **Choose File**.

Step 10 Click **Next**.

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

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

Note Cisco Prime Collaboration Deployment does not allow you to select the date and time for the dependent tasks, as the dependent task starts automatically after the successful completion of the existing task.

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

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

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

  Note If you choose to start the task manually, a task is created, but does not start until you click the **Start task** button on the Monitoring page, or the **Start task** link on the task page.

- Select **Start task immediately upon completion of this wizard** to start the task immediately after you click **Finish**.
- If you want the system to automatically switch to the new version, choose the option **Upgrade Option to Automatically Switch to New Version after Successful Upgrade**. Otherwise, the server, or servers, are upgraded but remain on the current version of software. In that case, you can schedule a switch version task to switch over to the upgraded version of software.

Step 12 Click **Next**.

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

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.

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

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

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

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

Step 14 Click **OK**.

Step 15 Click **Next**.

Note The **Next** button remains enabled, which allows you to click to display any configuration errors.

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

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

Related Topics

Supported Tasks for Applications and Versions, on page 4
Upgrade Paths for Export Restricted and Unrestricted Software, on page 9

Direct Refresh Upgrade

You can perform refresh upgrade to upgrade from existing version of a product to a later version where operating systems of both the versions are different. The supported products for this upgrade are Cisco Unified Communications Manager, IM and Presence Service, Cisco Unity Connection, Cisco Unified Contact Center Express, and .

In the earlier releases, after direct refresh upgrade, although Cisco Unified Communications Manager was upgraded to the new version, it used to switch back to its older version. The new version used to be an inactive version. For the new version to be the active version, switch version was required. The switch back used to happen because upgrade and switch version were two separate steps. It implies that the version had to be switched twice to make the new version after direct refresh upgrade.

To prevent switch version twice, in this release, Cisco Prime Collaboration Deployment includes switch version step as part of upgrade step during refresh upgrade. Check the **Automatically switch to new version after successful upgrade** check box in the **Upgrade Task** window during upgrade task configuration. Then,

the switch version of the product (either Cisco Unified Communications Manager or IM and Presence Service) is included as part of the upgrade step. However, the switch version step appears as a separate step if the upgrade is for Cisco Unified Communications Manager and IM and Presence Service cluster.

Database Replication

Database replication is one of the steps of refresh upgrade process. Cisco Prime Collaboration Deployment runs services and commands and waits for the database replication status of the selected Cisco Unified Communications Manager nodes.

For more information, see "Sequencing Rules and Time Requirements" chapter of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.

Note Cisco Prime Collaboration Deployment checks the database replication when you choose the cluster that is combined with Cisco Unified Communications Manager and IM and Presence Service. The database replication runs only for Cisco Unified Communications Manager before the IM and Presence Service upgrade or switch.

Only after successful database replication, the next task that is listed in the upgrade sequence starts. The tasks listed after database replication include upgrade or switch version of IM and Presence Service subscriber nodes.

Reuse Sequence from Previous Task

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

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

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

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

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

Switch Versions Task

Create a Switch Versions Task

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

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

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

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

Note The Automatic Switch version option is not available on clusters which contain Unity Connection 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.

Before you begin

1. Perform a cluster discovery for the cluster on which you want to switch versions, so that the cluster appears in the Cluster inventory. See Discover a Cluster, on page 10. If you previously used Cisco Prime Collaboration Deployment to upgrade or migrate a cluster, the cluster should already be in the inventory.
2. For each application server in the cluster, ensure that the Platform Administrative Web Service is active on that server.

Procedure

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

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

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

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

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

Step 5 Click **Next**.

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

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

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

- Select **Start task manually** to keep the task in a manual start.
- Select **Start task immediately upon completion of this wizard** to start the task immediately after you click **Finish**.

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

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

Step 7 Click **Next**.

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

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

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

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

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

Step 9 Click **OK**.

Step 10 Click **Next**.

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

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

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

Related Topics

Supported Tasks for Applications and Versions, on page 4
Upgrade Paths for Export Restricted and Unrestricted Software, on page 9

Server Restart Task

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

Related Topics

Supported Tasks for Applications and Versions, on page 4
Upgrade Paths for Export Restricted and Unrestricted Software, on page 9

Create a Server Restart Task

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

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

Before you begin

1. Perform a cluster discovery for the cluster you wish to restart, so that it appears in the Cluster inventory. See Discover a Cluster, on page 10.
2. For each application server in the cluster, ensure that the Platform Administrative Web Service is active on that server.
3. If you are using Cisco Prime Collaboration Deployment Readdress Task with virtual machine of an application, ensure that you follow the application's rules for changing IP and hostname—either one at a time or simultaneously.

Procedure

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

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

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

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

Step 5 Click **Next**.

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

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

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

- Select **Start the task manually** to keep the task in a manual start.
- Select **Start task immediately upon completion of the wizard** to start the task immediately after you click **Finish**.

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

Step 7 Click **Next**.

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

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

- The Pencil icon opens up an **Edit Step** window. In this step, add nodes to be restarted from the list of available nodes. The available nodes are the ones that you chose for a restart.
- The step to which each node is assigned appears next to the node. If a node is not assigned to any step, that node shows as unassigned.
- When you assign all the nodes to a step, a default sequencing is available.

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

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

Step 9 Click **OK**.

Step 10 Click **Next**.

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

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

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

Readdress Task

Create a Readdress Task

Use the readdress task change the hostname or IP address for one or more nodes in a cluster. To use the readdress feature, the servers must be Release 11.5 or later.

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

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

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

Before you begin

- If you have not already done so, perform a cluster discovery for the cluster you wish to readdress, so that it appears in the Cluster inventory. See Discover a Cluster, on page 10.
- If you are using Cisco Prime Collaboration Deployment Readdress Task with virtual machine of an application, ensure that you follow the application's rules for changing IP and hostname—either one at a time or simultaneously.

Procedure

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

Step 2 Click **Add Readdress Task**.

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

Step 4 Click **Next**.

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

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

Step 6 Click **OK**.

Step 7 Click **Next**.

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

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

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

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

- Select **Start task manually** to keep the task in a manual start.
- Select **Start task immediately upon completion of wizard** to start the task immediately afer you click **Finish**.

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

Step 9 Click **Next**.

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

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

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

Note IM and Presence Service nodes do not have an **Edit** button, since readdress is not supported on Cisco Prime Collaboration Deployment for IM and Presence Service servers.

- The step to which each node is assigned displays next to the node. If a node is not assigned to any step, it shows as unassigned.
- When you assign all the nodes to a step, there will be a default sequencing available.

Important You cannot proceed to next step until you assign all the nodes that were selected for this task.

- Cisco Prime Collaboration Deployment automatically inserts a Forced Pause after each sequence step in a Readdress task.
- For a readdress task, only one node can be assigned to each step. Multiple nodes cannot be combined and assigned in a single step.

Step 11 Click **OK**.

Step 12 Click **Next**.

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

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

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

Run a Readdress Task

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

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

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

The forced pause allows you to perform manual steps, such as updating DNS entries and server entries on the Unified Communications publisher node interface (**System** > **Server**). It also allows you to check the phones associated with the server successfully registered. User needs to perform these steps before resuming the readdress task in the interface for other Unified Communications nodes as well. After the readdress task resumes, the system replicates the updates successfully.

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

Before you begin

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

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

Post Readdress Task

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

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

Install Task

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

Create an Install Task

Before you begin

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

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

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

Note The ISO file must be bootable.

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

3. VMware—Deploy Cisco-recommended OVA to create the VMs for the nodes to be installed. Create the appropriate number of target virtual machines on your ESXi hosts (one new virtual machine for each server to be installed in the cluster) using the Cisco OVAs that you downloaded in Step 2. Configure the network settings on new VMs.
4. Cisco Prime Collaboration Deployment GUI—Add the ESXi Hosts that contain your virtual machines to the Cisco Prime Collaboration Deployment inventory. For information about adding and ESXi host to Cisco Prime Collaboration Deployment, see Add an ESXi Host Server, on page 13.
5. Cisco Prime Collaboration Deployment GUI—Define the new installation cluster (click the open and close navigation button and choose **Inventory** > **Clusters**) to define the nodes to be installed, and their associated virtual machines. (See Add New Cluster for Fresh Install, on page 16.)
6. Cisco Prime Collaboration Deployment GUI—Setup Email Notification (Optional)
   - Click the open and close navigation button and choose **Administration** > **Email Notification**.
   - When email notification is set up, the Cisco Prime Collaboration Deployment server emails the error conditions that may occur during the migration task.
7. Cisco Prime Collaboration Deployment GUI—Create the Install task.
8. Be sure to enter the IP addresses or hostnames of the cluster nodes to be installed into your DNS server before you create the install task.

Add Install Task

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

Procedure

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

Step 2 Click **Add Install Task**.

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

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

Step 4 Click **Next**.

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

Important The ISO file is visible here only if it was placed in the local SFTP directory under `/fresh_install`, if Prime Collaboration Deployment is used as local SFTP. If any remote SFTP is associated with the migration cluster, then the files should present in the remote SFTP. For more information, see the task management information at the beginning of this section.

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

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

Note When you add the Remote SFTP server, you should maintain the different SFTP directories for fresh install/migration and upgrade. You can add the same Remote SFTP server for fresh install/migration and upgrade but directories for fresh install/migration and upgrade should be different.

Step 6 Click **Choose File**.

Step 7 Click **Next**.

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

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

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

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

- Select **Start task manually** to keep the task in a manual start.
- Select **Start task immediately upon completion of this wizard** to start the task immediately after you click **Finish**.

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

Step 9 Click **Next**.

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

Option	Description
Pencil icon	Edit a step.
Page icon	Add a new step after the current step.
X mark	Delete the current step.

Option	Description
	If you remove all the nodes from a step, the step is removed by default. You cannot remove a step that contains the Publisher node.
Up arrow	Move the step up to be performed earlier.
Down arrow	Move the step down to be performed later.

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

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

- If you are installing Cisco Unified Communications Manager between Releases 10.0(1) and 10.5(1), the task is paused after publisher node is installed completely. You must enter details of subscriber nodes into the publisher node before you manually start the next step. Cisco Unified Communications Manager Release 10.5(2) onward does not pause during a fresh installation; the install task continues automatically.

Step 11 Click **OK**.

Step 12 Click **Next**.

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

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

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

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

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

Run an Install Task

If you scheduled a task to start at a later date or if you chose Manual Start, the task is listed in the Task list, but has not started yet. In this case, a validation button is associated with the install task. Click **Validation** to check the task before you run it. By running validation before you start the task, you are alerted to any potential

problems with the task (such as a missing ISO file or VMs not in the Off state). You can then fix these issues before you start the task.

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

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

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

After all the subscribers to be installed in this cluster (Unified Communications Manager subscribers, IM and Presence Service publisher and IM and Presence Service subscribers) are added to the Unified Communications Manager publisher GUI, return to the Monitoring page in the Cisco Prime Collaboration Deployment GUI and click the **Resume** button for the install task to resume. The install task continues and installs the Unified Communications Manager or IM and Presence Service software on the subsequent server (or servers).

Cancel Install Task

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

Procedure

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

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

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

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

Post-Install Task

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

Edit and Expand Cluster Support

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

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

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

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

Edit or Delete a New Install Cluster

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

Procedure

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

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

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

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

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

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

Note Before you enable FIPS mode, Common Criteria, or Enhanced Secuirty Mode, ensure that you have minimum 14 characters for Security Password.

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

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

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

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

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

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

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

The changes are saved. You can install one or multiple nodes in a cluster. See Add Install Task, on page 43 for details.

Edit or Delete a Discovered Cluster

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

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

Note The fields in this section are non-editable.

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

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

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

The changes are saved. You can install one or multiple nodes in a cluster. See Add Install Task, on page 43 for details.

Monitor Task Status

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

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

Procedure

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

Step 2 The column on the left side of the Monitoring page lists each task and an icon that shows its current status. Also shown is the type of task (Migrate, Upgrade, Install, and so on), and the cluster nickname for the task.

The task start time is also shown. Click the task in this left column to view the detailed data for that task in the panel on the right.

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

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

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

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

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

Step 4 The bottom right section of the page provides detailed steps for the task, along with the status for that step. Click on the triangle that corresponds to a step to expand the step description.

Each step also has a View Log link, to show the log messages for that step.

Note The Monitoring page refreshes automatically every 6 minutes. To deactivate automatic refresh, click the **Disable** button.

Action Buttons on the Monitoring Page

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

Automatic Refresh

The Monitoring page refreshes automatically every 6 minutes. To deactivate automatic refresh, click the **Disable** button in the top left corner of the Monitoring page.

Administration Tools

Email Notification

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

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

When Email Is Sent

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

- Scheduled

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

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

- Failed to Schedule
- Failed
- Failed to Cancel
- Paused on Error

If PCD task of X steps, operating on 1 to N nodes the task action you get, email notifications when each node/task step is completed

Migration Task:

- Task Scheduled for Cluster
- Task Started for Cluster
- Source Node(s) A Configuration export success
- Source Node(s) B Configuration export success
- Destination Node(s) A Install success
- Destination Node(s) B Install success
- Source Node(s) A UFF Export success
- Source Node(s) A shut down success
- Destination Node(s) A UFF Import success
- Source Node(s) B UFF Export success
- Source Node(s) B shut down success
- Destination Node(s) B UFF Import success
- Task Completed/Failed

Upgrade Task (COPs):

- Task Scheduled for Cluster
- Task Started for Cluster
- COPs x installed on node a
- COPs y installed on node b
- Task Completed/Failed

PCD Fresh Install Task or Upgrade Task (ISO):

- Task Scheduled for Cluster
- Task Started for Cluster
- Node(s) A has been complete
- Node(s) B has been complete
- Task Completed/Failed

PCD Restart Task:

- Task Scheduled for these nodes
- Task Started for these nodes
- Node(s) A has been restarted
- Node(s) B has been restarted
- Task Completed/Failed

PCD Switch Version Task:

- Task Scheduled for these nodes
- Task Started for these nodes
- Node(s) A has been switched
- Node(s) B has been switched
- Task Completed/Failed

PCD Readdress:

- Task Scheduled for these nodes
- Task Started for these nodes
- Node(s) A has been readdressed
- Node(s) B has been readdressed
- Task Completed/Failed

SFTP Datastore

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

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

Migration or Fresh Install Tasks

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

Procedure

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

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

Example:

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

Step 3 Upload the ISO file.

Example:

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

Upgrade Task

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

Procedure

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

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

Example:

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

Step 3 Upload the ISO file or COP file.

Example:

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

Verify or View an ISO Filename

Procedure

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

Step 2 On this page, you can view and manage files that are stored on the SFTP datastore of this Cisco Prime Collaboration Deployment server.

It displays the filename of the ISO and COP files that are stored on the server, and where they are located in the directory (for example: fresh_install or upgrade).

Delete ISO or COP Files

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

Procedure

Step 1 Log in to Cisco Prime Collaboration Deployment.

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

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

Step 4 Click **Delete**.

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

Remote SFTP Server Support

The remote SFTP server support feature leverages Cisco Prime Collaboration Deployment for upgrades, migrations, and fresh installs. Use of this feature avoids the issues that are caused by large application image files streamed over WAN that are only supported by Cisco Prime Collaboration Deployment 12.1(1) and later.

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

- Geographically distributed deployments, such as multi-site distributed IP Telephony with multiple clusters at separate sites from the Cisco Prime Collaboration Deployment virtual machine.
- Clustering over WAN (CoW), where the application virtual machines are at different sites than the Cisco Prime Collaboration Deployment virtual machine.

- Deployments where Cisco Prime Collaboration Deployment is in central data center; however Cisco Unified Communications Manager clusters are remote over the WAN.

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

- Open SSH
- Cygwin
- Titan

Note The remote SFTP server support is available for upgrade, migration, and fresh install tasks.

Add Remote SFTP Server

Before you begin

For migration or fresh install, mount the remote SFTP server to be used as NFS on the ESXi host manually.

Procedure

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

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

Step 3 Click **Install/Migration** or **Upgrade** radio button.

Step 4 In the **Address and access credentials** section, enter values in the **IP / Host Name**, **Username**, and **Password** fields.

Step 5 For Install or Migration task type, in the **Remote NFS Path to Datastore Directory on Server** section, enter the directory path in **Directory** field and NFS server name in **NFS Server Name** field.

Feild	Description
Directory	Path which has been configured for NFS storage in ESXI host.
NFS Server Name	Name of NFS storage which has been created in ESXI.

Example:

Directory: /abc/def/

NFS Server Name: xyz_NFS

When adding an NFS server, the SFTP credentials should point to a directory that is an exact match for the path which is configured in the ESXi host. For more information on adding NFS storage in EXSI host refer the respective documentation guide.

Step 6 For Upgrade task type, in the **Remote SFTP Path to Datastore Directory on Server**, click an **Add Directory** button to add a value in the **Directory** field.

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

Step 7 (Optional) In the **Additional Information** section, enter description in the **Description** field.

Step 8 Click **Add**.

Upon the successful add of remote SFTP server for the install or migration task type, a dialog box is displayed. Dialog box lists the ESXi hosts which are already added to Prime Collaboration Deployment under **Inventory** > **ESXi Hosts** that has the given NFS directory mounted.

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

- **Connection Timeout**—Indicates that the connection to SFTP server failed due to timeout.
- **Login Failure**—Indicates that the login to the SFTP server failed.
- **Directory Not Found**—Indicates that the directory that you selected is not found on the SFTP server.
- **Directory Already Entered**—Indicates that the directory that you selected already exists in the list of directories. You can view the list of available directories by clicking the **Add Directory** button.
- **Directory Already Exists**—Indicates that the directory that you entered already exists in the list of the SFTP servers.
- **Mandatory Fields Missed**—Indicates that you did not enter values in the mandatory fields.
- **Mentioned Server Could Not Be Located**—Indicates that the server that you entered is not configured with DNS. This error message appears if you enter host name instead of IP address.
- **No ESXi Hosts in Inventory**—Indicates that you have not added ESXi hosts. This error appears when you try to add Install or Migration task type remote SFTP, and the given NFS mount is not found as there are no ESXi hosts added under **Inventory** > **ESXi Hosts** page.
- **Could not find given NFS path/Directory on the listed ESXi host(s) under Inventory** > **ESXi Hosts**—This error appears when you try to add Install or Migration task type remote SFTP, and the given NFS directory is not found in any of the ESXi which are added under **Inventory** > **ESXi Hosts** page.

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

Associate Nodes to Remote SFTP Server

Before you begin

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

Procedure

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

Step 2 Click **Discover Cluster** button to search for the existing clusters. To discover a cluster, see the Discover a Cluster, on page 10 procedure.

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

Step 4 From the **SFTP Server** drop-down list, choose an SFTP server.

By default, this field shows the `localhost` option as the SFTP Server.

Step 5 Click **OK**.
The SFTP server is associated with the cluster node that you selected and the details appear in the **SFTP Server** column of the **Cluster Nodes** table.

Edit Remote SFTP Server

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

Before you begin

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

Procedure

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

Step 2 From the available SFTP servers in the **SFTP and NFS File access** table, click **Edit** for an SFTP server.
The **Edit SFTP Server** window appears.

Step 3 For Install or Migration tasks, edit the values for the fields in the **Address and access credentials**, **Remote NFS Path to Datastore Directory on Server**, **NFS Server Name** , and **Additional Information** sections.

Upon successful edit of remote SFTP server for install or migration task type, a dialog box is displayed. Dialog box lists the ESXi hosts which are already added to Prime Collaboration Deployment under **Inventory** > **ESXi Hosts** that has the given NFS directory mounted.

Step 4 For Upgrade task, edit the values for the fields in the **Address and access credentials**, **Remote SFTP Path to Datastore Directory on Server**, and **Additional Information** sections.

In **Remote SFTP Path to Datastore Directory on Server** section, by clicking the **Add Directory** button, you can edit an existing directory and also add multiple directories.

Step 5 Click **Save**.

Delete Remote SFTP Server

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

Before you begin

- Ensure that no install, migration or upgrade tasks are associated and running with the cluster node that uses the SFTP server that you choose to delete.
- Disassociate the cluster nodes from the SFTP server that you choose to delete.

Note You can disassociate a cluster node even if no install, migration or upgrade tasks are associated and running with the cluster node that uses the SFTP server that you selected to delete.

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

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

Procedure

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

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

Step 3 Click **Delete**.

Delete Local SFTP/Datastore ISO files

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

Before you begin

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

Procedure

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

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

Note You cannot delete remote SFTP files.

Step 3 Click **Delete**.

Disk Space Warning Level

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

Configure Disk Space Warning Level

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

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

Procedure

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

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

Step 3 Enter the value that you want to assign for the **Warning Level Disk Space (GB)** field.

You can click the information link to check if the space value you entered is available for use on the server.

Step 4 Click **Save**.

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

Audit Log Configuration

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

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

Configure Audit Logs

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

Procedure

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

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

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

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

- When you check this field, the audit events are logged in the local server. When you uncheck this field, audit events are not logged in the local server. The audit events includes User ID, ClientAddress, Severity, EventType, ResourceAccessed, EventuStatus , AuditCategory, CompulsoryEvent, ComponentID, CorrelationID and Node ID.
- When you check this field, the **Enable Log Rotation** field becomes active.

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

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

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

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

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

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

Step 9 Click **Save**.

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

Customized Logon Message

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

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

Configure Customized Logon Message

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

Procedure

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

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

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

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

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

FIPS 140-2 Compliance

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

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

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

For details on EnhancedSecurityMode, see EnhancedSecurityMode Support, on page 62.

Note

- Elliptic Curve Digital Signature Algorithm (ECDSA) ciphers are not supported in Cisco Prime Collaboration Deployment. Hence, during TLS connection, the server does not negotiate the ECDSA certificates even though the **show cert list own** CLI command may show the ECDSA self-signed certificate.
- All the nodes of a cluster should either be FIPS or non-FIPS.

EnhancedSecurityMode Support

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

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

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

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

Note If you configure UC clusters on FIPS mode or EnhancedSecurityMode, ensure that you also configure Cisco Prime Collaboration Deployment with the similar modes. With this configuration, you can run the tasks that are specific to UC clusters.

Credential Policy for EnhancedSecurityMode

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

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

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

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment

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

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

Audit Framework and Audit Activities

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

You can configure these details from the following options:

- **Logout** button
- **Email Notification** window
- **NAT Settings** window
- **Disk Space Configuration** window
- **Audit Log Configuration** window
- **Customized Logon Message** window

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

EnhancedSecurityMode Requirements for Platform Cisco Prime Collaboration Deployment

You can use the command line interface (CLI) to enable EnhancedSecurityMode in Cisco Prime Collaboration Deployment.

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

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

Note For credential policy for EnhancedSecurityMode, see Credential Policy for EnhancedSecurityMode, on page 63.

Re-encryption through AES

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

Limited Number of Sign-in Sessions

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

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

set session maxlimit <value>

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

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

Minimum TLS Version Control

This release of Cisco Prime Collaboration Deployment includes the minimum Transport Layer Security (TLS) protocol version configuration support. Use this feature to configure the minimum TLS version to comply with the organization security policies.

The supported TLS versions are TLS 1.0, 1.1, and 1.2. By default, TLS 1.0 is configured. After you configure the minimum TLS version, both the minimum version and the higher versions are supported.

Before you configure the minimum TLS version, ensure that the following products support secure connection of the selected minimum TLS version configured or above. If this requirement is not met, upgrade the product to a version that supports the interoperability for selected minimum TLS version configured or above when you configure the minimum TLS version.

- Cisco Unified Communications Manager
- IM and Presence Service
- Cisco Unity Connection
- Cisco Unified Contact Center Express
-

To configure the minimum TLS version, see the CLI Commands for TLS Minimum Version Configuration topic.

Configurable Maximum Install Timeout for Clusters

With this release, you can configure the maximum timeout value during the migration of nodes of a cluster. In the previous releases, the default timeout value from Cisco Prime Collaboration Deployment was 5 hours for both install and migration tasks. This restriction prevented the nodes that have large data to import during migration to time out from Cisco Prime Collaboration Deployment side.

You can configure the maximum timeout value from the **Max Timeout for Install** drop-down list on the **Configure Destination Cluster** window. Click **Inventory** > **Clusters** to access the **Configure Destination Cluster** window. When you configure a migration destination cluster, you can choose the maximum timeout value for **Max Timeout for Install** from 5 hours up to 10 hours.

Note For Install task, Cisco Prime Collaboration Deployment has the default timeout value as 5 hours, which is non-configurable.