Install Cisco Prime Collaboration Deployment

System Requirements for Installation

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

Table 1: Cisco Prime Collaboration Deployment Installation Server Requirements

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

Browser Requirements

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

Note Other browsers are not supported.

Cisco Prime Collaboration Deployment supports the following operating system browsers:

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

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

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

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

IP Address Requirements

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

Virtualization Software License Types

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

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

Note Cisco Business Edition 6000 and Cisco Business Edition 7000 servers are preinstalled with Cisco UC Virtualization Hypervisor. If you plan to use Cisco Prime Collaboration Deployment with application VMs on these servers, you must substitute a higher virtualization software feature level.

The following are compatible with Cisco Prime Collaboration Deployment:

- Cisco UC Virtualization Foundation 6x (appears as “Foundation Edition” in vSphere Client)
- Cisco UC Virtualization Hypervisor Plus 6x
- Cisco Collaboration Virtualization Standard 6x
- Cisco Collaboration Virtualization Standard 6.4 or higher
- VMware vSphere Standard Edition 6x
- Evaluation mode license

  (for example, for lab deployments and not production use)

The following are not compatible with Cisco Prime Collaboration Deployment:

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

Frequently Asked Questions About the Installation

Review this section carefully before you begin the installation.

How Much Time Does the Installation Require?

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

What Usernames and Passwords Do I Need to Specify?

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

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

- Administrator account username and password
- Security password

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

- Cisco Prime Collaboration Deployment GUI interface
- Command line interface

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

- Administrator account username—Must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.

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

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

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

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

What Is a Strong Password?

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

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

Avoid the following types of passwords:

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

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

Can I Install Other Software on the Virtual Machine?

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

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

Preinstallation Tasks

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

Table 2: Preinstallation Tasks

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

Allow Network Traffic

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

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

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

Table 3: Corporate Firewall Configuration

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

Direction	Source	Destination	Protocol	Port	Description
Inbound	Cisco Prime Collaboration Deployment	IP address of the sftp server	TCP	22	SFTP access to Cisco Prime Collaboration Deployment server for uploading licenses and software, upgrade, and CLI access
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTP	80	HTTP access to nonsecured GUI and web APIs (for example, login page)
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	111	Network File System
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTPS	443	HTTPS access to secured GUI and web APIs
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	662	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	892	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	TCP/UDP	2049	Network File System
Inbound	UC application servers	Cisco Prime Collaboration Deployment server IP address	HTTPS	6060	Asynchronous SOAP messages from application servers
Inbound	Internal network or any management workstation	Cisco Prime Collaboration Deployment server IP address	HTTPS	8443	HTTP alternate

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

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

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

Gather Information for Installation

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

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

⚠

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

Table 5: Server Configuration Data

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

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

Parameter	Description	Can Entry Be Changed After Installation?
Hostname	Enter a hostname that is unique to your server. The hostname can consist of up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen. **Important** Do not change your hostname while any tasks are running.	Yes, you can change the entry after installation. **set network hostname** **Note** On hostname change, make sure to re-mount the Prime Collaboration Deployment NFS on all the ESXi hosts which were added to the Prime Collaboration Deployment. This can be done by the following: **1.** Login to each ESXi host which was added to Prime Collaboration Deployment. **2.** Right-click on the Prime Collaboration Deployment NFS storage and delete it. **3.** From the Cisco Prime Collaboration Deployment application, click the open and close navigation button, and choose **Inventory** >**ESXi Hosts**. **4.** Click **Edit** on each ESXi host and click **OK**. This will remount the Prime Collaboration Deployment as NFS on the respective ESXi host with updated hostname.
IP Address	Enter the IP address of your server.	Yes, you can change the entry after installation. **set network ip eth0**

Parameter	Description	Can Entry Be Changed After Installation?
IP Mask	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: **set network ip eth0**
Location	Enter the location of the server. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: **set web-security**
MTU Size	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host transmits on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. The default value is 1500 bytes.	Yes, you can change the entry after installation by running the following CLI command: **set network mtu**
NTP Server	Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Caution** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node can be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.	Yes, you can change the entry after installation by running the following CLI command: **utils ntp server**

Parameter	Description	Can Entry Be Changed After Installation?
Organization	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry.	Yes, you can change the entry after installation by running the following CLI command: **set web-security**
Security Password	Enter your security password. The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password. **Note** Before you enable FIPS mode, Common Criteria, or Enhanced Security Mode, ensure that you have a minimum 14 characters for Security Password.	Yes, you can change the entry after installation by running the following CLI command: **set password user security**
State	Enter the state in which the server is located.	Yes, you can change the entry after installation by running the following CLI command: **set web-security**
Time Zone	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by running the following CLI command: **set timezone** To view the current time zone configuration, run the following CLI command: **show timezone config**

Begin Installation

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

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

Table 6: Installation Wizard Navigation

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

Install Cisco Prime Collaboration Deployment

Extract the PCD_VAPP.OVA File

Cisco Prime Collaboration Deployment is delivered with Unified Communications Manager, through a new purchase or an entitled upgrade that you access through the My Cisco Entitlements (MCE).

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

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

Procedure

Step 1 Extract the PCD_VAPP.OVA from the pcd_vApp_UCOS_10.xxxxx.iso file.

A new PCD_VAPP.OVA file is created. Verify the file size; ISO and OVA files do not have the same file size.

Step 2 Deploy the PCD_VAPP.OVA file in vCenter to install Cisco Prime Collaboration Deployment.

If you are using the vSphere client, the name of this file may be PCD_VAPP.OVA. If you are using the VMware vSphere web client to deploy the file, you must first change the name to PCD_VAPP.ova (lowercase) before you deploy the file.

Install the Virtual Machine

Before you begin

- Download the OVA image.

  Note If you are using Cisco Business Edition 6000 or Cisco Business Edition 7000 appliance with factory preloaded Cisco Collaboration Systems Release 11.5 or higher, you need not download the OVA image. The Cisco Prime Collaboration Deployment OVA is available in the datastore of the appliance. For details, see http://www.cisco.com/c/en/us/products/unified-communications/business-edition-6000/index.html or http://www.cisco.com/c/en/us/products/unified-communications/business-edition-7000/index.html.

- Read the "Preinstallation Tasks" section.

- Place a copy of the OVA on your local drive, depending on the installation type you are using.

Installation Type	Filename	Used with ESXi Host Software Version
OVA	PCD_VAPP.OVA or PCD_VAPP.ova **Note** The name of the OVA file depends on whether you are using vSphere client or VMware vSphere web client to deploy the file. For more information, see Extract the PCD_VAPP.OVA File, on page 13	6.5 and above

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

Procedure

Step 1 Log in to vCenter.

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

Step 3 Specify the location of the OVA file and click **Next**.

The **OVF Template Details** window opens and the product information is displayed, including the size of the file and the size of the VM disk.

Step 4 Click **Next**.

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

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

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

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

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

Step 10 Review the options that you selected, and if no changes are required, click **Finish** to begin the OVA installation.

After the installation is complete, the newly installed virtual machine appears in the selected location within vCenter.

Configure Cisco Prime Collaboration Deployment on the Virtual Machine

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

Procedure

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

Step 2 Power on the virtual machine.

Installation begins automatically.

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

The **Platform Installation Wizard** screen appears.

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

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

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

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

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

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

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

Step 10 If you chose not to use DHCP, enter your static network configuration values and click **OK**.

The DNS Client Configuration window appears.

Step 11 To enable DNS, click**Yes**, enter your DNS client information and click **OK**.

The network restarts by using the new configuration information, and the **Administrator Login Configuration** window appears.

Step 12 Enter your Administrator username and password.

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

Step 13 Enter the Certificate Information:

- Organization
- Unit
- Location
- State
- Country

Step 14 Click **OK** to proceed.

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

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

Step 17 When asked, enter your security password.

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

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

Postinstallation Tasks

Procedure

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

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