Post Installation Tasks

Log in to Cisco Prime Collaboration Provisioning

You can invoke Cisco Prime Collaboration using the client browser.

Before you begin

Ensure that you have a browser that supports Cisco Prime Collaboration Provisioning. For more information on supported browsers, see System Requirements.

Procedure

Step 1 Open a browser session from your machine. .

For a standalone mode, Specify the IP address of the Cisco Prime Collaboration Provisioning application.

Step 2 Enter either of the following:`http://IP Address` or `https://IP Address`

Note

- For Cisco Prime Collaboration Assurance, HTTPS has been enabled by default; whereas, for Cisco Prime Collaboration Provisioning, HTTP has been enabled by default.

  To enable HTTPS for Cisco Prime Collaboration Provisioning, configure OpenSSL packages that are packaged with the Cisco Prime Collaboration Provisioning OVA. See Enabling SSL for Prime Collaboration Provisioning.

- You can use either the IP address or the hostname of the Cisco Prime Collaboration Provisioning server. We recommend that you use the hostname if you have configured it in DNS.

- Troubleshooting Account CLI is supported only through SSH; Telnet is not supported. The port used for Cisco Prime Collaboration Provisioning is 22.

Based on the browser you are using, you see one of the following:

- In Windows Internet Explorer, **the Certificate Error: Navigation Blocked** window.
- In Mozilla Firefox, **the Untrusted Connection** window.
- In Google Chrome, **the Privacy Error: Connection is not private** window.

These windows appear because Cisco Prime Collaboration uses a self-signed certificate.

Step 3 Remove the SSL certificate warning.

The **Cisco Prime Collaboration login** page appears.

Step 4 In the **Cisco Prime Collaboration login** page, you must log in for the first time as a global administrator, using the same credentials that you specified during the installation.

The dashboard data is populated only after you perform tasks listed in the following table.

Get Started with Cisco Prime Collaboration Provisioning

After you install Cisco Prime Collaboration Provisioning, perform the tasks listed in the following table:

	Task and Description	**Navigation in Cisco Prime Collaboration Provisioning Application**	**Reference Section/Chapter in** Cisco Prime Collaboration Provisioning Guide - Standard and Advanced
Step 1	(Optional if you are evaluating the product or have installed the product in standard mode) Register a new license file.	**Administration** > **License Management** We recommend that you add a license file through the user interface. 1. **Administration > License Management > Add License Files** The system validates the license file and updates the license. The updated licensing information appears on the **License Status Information** window (**Administration** > **License Management**). **Note** If the license status is not refreshed after a few minutes, manually refresh the **License Management** window to view the updated license status.	Setting Up the Server

	Task and Description	Navigation in Cisco Prime Collaboration Provisioning Application	Reference Section/Chapter in Cisco Prime Collaboration Provisioning Guide - Standard and Advanced
Step 2	Add, configure, and synchronize call processors and message processors.	**Infrastructure Setup** > **Getting Started Wizard** **Infrastructure Setup** > **Infrastructure Configuration**	Managing Devices
Step 3	Set up domain deployment: • Create domains and assign call and message processors • Create service areas • Configure rules • Synchronize domain	**User Provisioning**	Managing Domains and Service Areas Synchronizing Processors, Users, and Domains Managing Users
Step 4	Create and deploy templates to configure Cisco Unified Communication Manager or infrastructure configuration.	**User Provisioning**, or **Infrastructure Setup** > **Configuration Template**	Configuring Templates in Provisioning
Step 5	Assign user roles to a service area.	**Provisioning Setup** > **Domain** > **Service Area** > **Edit**	Managing Users
Step 6	Add a new user.	**User Provisioning** > **Add**	Managing Users
Step 7	Provision user services.	**User Provisioning**	Managing Orders

Verify Cisco Prime Collaboration Provisioning Installation

Perform the following procedure to verify whether Cisco Prime Collaboration Provisioning is installed properly.

Verify Cisco Prime Collaboration Provisioning Installation 11.x

Procedure

Step 1 In a browser, specify the IP address of the server on which Cisco Prime Collaboration Provisioning (standard or advanced) is installed. The login page is displayed. Log in with global administrator credentials.

Step 2 Log in to the Provisioning server using the SSH service and with the CLI administrator that you created during OVA configuration. By default, this username is admin.

Step 3 Display the processes that are running.

show application status cpcm

bash : no job control in this shell httpd denotes httpd service

nice.sh denotes Nice service

startcupm.sh denotes Jboss service

postmaster/su denotes Postgres service

```
STAT PID USER COMMAND ELAPSED
==============================================
Ss 629 root httpd 02:11:38
S 613 root nice.sh 02:11:38
S 610 root startcupm.sh 02:11:38
S 608 root su 02:11:38
```

The parameters in the COMMAND column are the processes that are running on the Cisco Prime Collaboration Provisioning server (standard or advanced). If you do not see the processes running, enter the following commands to restart the Cisco Prime Collaboration Provisioning services:

admin#application stop cpcm

admin#application start cpcm

These commands take one or two minutes to stop or start the Cisco Prime Collaboration Provisioning services.

Step 4 You can verify if the installation is complete and successful, by checking if the JBoss service is running. In the SSH terminal, run the following command:

ps - aef|grep startcupm

You can also check at what time the JBoss service was started, in the following location (in the last line of the log file):

```
/opt/cupm/sep/logs/jboss.log
```

If the JBoss service is running, see Log in to Cisco Prime Collaboration Provisioning, to get started with the Cisco Prime Collaboration Provisioning application.

Verify Cisco Prime Collaboration Provisioning Installation 12.x

Procedure

Step 1 Log in to the Cisco Prime Collaboration Provisioning server as globaladmin.

Step 2 Go to **Administration** > **Logging and Showtech**.

Step 3 Create a troubleshooting user, and obtain the response string by mailing challenge string to the Engineering Team.

Step 4 Log in as troubleshooting user to the Troubleshooting UI.

With the Troubleshooting UI, the user can check the services, create the console account, and access the Prime Collaboration Provisioning CLI.

Step 5 Go to **Administration** > **Process Management**.

Step 6 Verify if all the servers are running:

- Postgre SQL (Database)
- Apache (Web Server)
- JBOSS (Application Server)
- NICE (Configuration Engine)
- Troubleshooting Application

Generate Certificate Signing Request (CSR)

Procedure

Step 1 Go to micro service page, and then create a troubleshooting user. For creating a troubleshooting user, refer to Creating a Troubleshooting Account.

Step 2 Generate the Console Account, and then login to the CLI account.

Step 3 Go to **cd /opt/cupm/httpd/bin**

Step 4 To generate the CSR, enter:

```
./openssl req -new -key <keyName>.key -out <csrName>.csr
```

Step 5 Enter the appropriate details when prompted, such as:

```
Country Name: <Country>
State/Prov: <State>
Locality: <Locality>
Organization name: <Org>
Organizational unit name: <unit>
Common name: <hostname>.<companyname>.com
```

Step 6 The generated CSR is available in the location `/opt/cupm/httpd`.

Uninstall Cisco Prime Collaboration Provisioning

Procedure

Step 1 Log in to the vSphere Client and connect to the ESXi server that is running the virtual appliance that you want to uninstall.

Step 2 Right-click the application and choose **Power > Shut Down Guest** (or choose **Power Off**).

Step 3 Right-click the application and in the **Confirm Delete** window, choose **Delete from disk**.

Troubleshooting Account

For information on creating and accessing a troubleshooting account, see Create a Troubleshooting Account and Access Troubleshooting Account or Console Account.

Snapshot Revert in a Distributed Setup

For snapshot revert in a distributed setup, we recommend you to perform the following steps to avoid the inconsistent application behaviour such as Provisioning services not available as expected and blank UI on the Application server:

Note Snapshots of both database server and application server must have been taken at the same time.

CLI access through the console account must be enabled before taking the VM snapshots.

1. Revert the snapshot for the database server.
2. Revert the snapshot for the application server.
3. Reboot the application server instance on the VM and wait for the login page to display in the browser.

Note If **Access Denied** error is displayed, repeat step 3.