Troubleshooting

Verify the Cisco Prime Collaboration Assurance Installation (for Advanced and Standard Mode)

If you are unable to launch Cisco Prime Collaboration Assurance, it could be because the required processes are not running on the Cisco Prime Collaboration Assurance server.

To verify the process status, login to Cisco Prime Collaboration Assurance Serviceability User Interface.

You can view the Cisco Prime Collaboration Assurance processes that are running on the server. You can start or stop the processes apart from viewing the server.

Note You cannot start or stop an individual process. You can either Start or Stop all processes.

- **Start All Process** button appears only when all processes are stopped.
- **Stop All Process** button appears when all/some processes are running.
- A notification also appears once the processes are started or stopped.
- You can click on View Process Status Detail link to view the progress of starting / stopping the processes. The View Process Status Detail link appears only when the processes is being started or stopped.

Note The process status dashboard automatically refreshes every 6 seconds.

Step 1 Log in to the Assurance server using the SSH service and with the CLI admin that you created during OVA configuration. By default, the username is admin.

Step 2 Display the processes that are running.

show application status cpcm

The following is sample output of the status command, for Cisco Prime Collaboration Assurance- Advanced server:

```
S<l 11866 root Decap_main 13-01:10:20
S 11988 postgres postgres 13-01:10:18
S 12132 primea postmaster 13-01:10:07
Sl 12262 root emsam_mq 13-01:09:50
Sl 12327 root cpc_multiproclo 13-01:09:42
Sl 12362 root emsam_inventory 13-01:09:42
Sl 13141 root emsam_perfmonen 13-01:08:03
S<l 13222 root emsam_tomcat 13-01:07:53
Sl 13314 root emsam_poller 13-01:07:28
Sl 13448 root emsam_fault 13-01:07:07
Sl 13885 root emsam_troublesh 13-01:06:18
Sl 13919 root emsam_sessionmo 13-01:06:17
Sl 14733 root cpc_datapurge 13-01:04:31
Sl 14828 root cpc_segserver 13-01:04:26
Sl 15027 root cpc_qovmserver 13-01:04:15
Sl 15386 root cpc_pifserver 13-01:04:00
Sl 15539 root cpc_ipiudataser 13-01:03:47
Sl 15572 root cpc_srstserver 13-01:03:45
Sl 15974 root cpc_stserver 13-01:03:38
Sl 17685 root cpc_sshd 13-01:01:04
Sl 17724 root cpc_qovr 13-01:01:02
Sl 17746 root cpc_smdbmonitor 13-01:01:00
Sl 17792 root cpc_ipslaserver 13-01:00:57
```

```
Sl 17889 root cpc_toposerver 13-01:00:52

Sl 19542 root cpc_gpf 13-00:54:09
```

The following is the output of status command for Cisco Prime Collaboration Assurance- Standard server:

```
STAT PID USER COMMAND ELAPSED

==============================================

S<l 3086 root Decap_main 21:44:29

S 3204 postgres postgres 21:44:28

S 3335 primea postmaster 21:44:16

Sl 3378 root emsam_mq 21:43:59

Sl 3445 root cpc_multiproclo 21:43:51

Sl 3479 root emsam_inventory 21:43:51

Sl 4336 root emsam_perfmonen 21:42:23

S<l 4417 root emsam_tomcat 21:42:13

Sl 4592 root emsam_poller 21:41:49

Sl 4736 root emsam_fault 21:41:29

Sl 5976 root emsam_troublesh 21:40:38

[root@DragonSmokeTestStd bin]#
```

The parameters in the COMMAND column are the processes that are running on the Cisco Prime Collaboration Assurance server (Standard/Advanced). If you do not see all of these processes running, enter the following commands to restart the Cisco Prime Collaboration Assurance services:

<hostname>/admin#application stop cpcm

<hostname>/admin#application start cpcm

```
The application start cpcm/cpcmcontrol.sh start takes 10 to 15 minutes for
execution and application stop cpcm/cpcmcontrol.sh stop takes 10 minutes.
```

Step 3 Repeat Step 2 and check whether all the processes are running.

If all the required processes are still not running on the Cisco Prime Collaboration Assurance server or if you are unable to access the Cisco Prime Collaboration Assurance URL, contact TAC team.

If all the processes are running, see Get Started with Cisco Prime Collaboration Assurance.

Upgrade Cisco Prime Collaboration Assurance Deployment Model

To upgrade Cisco Prime Collaboration Assurance deployment model, first upgrade your hardware resources, such as, vRAM, vCPU, and vDisk. You must increase the disk size by adding a new vDisk of size equal to the required extra size. See the VMware documentation to upgrade or add the hardware resources.

Note

- Do not select existing vDisk and increase its size. Add a new vDisk.
- If you are using Cisco Prime Collaboration Assurance 10.6 or later release and/or Cisco Prime Collaboration Analytics 10.6 or later release, you must contact Cisco TAC team to get the root access to the Cisco Prime Collaboration Assurance server. The root access enables you to run the tuning script.

You must log in as root user and upgrade the Cisco Prime Collaboration Assurance deployment model to medium, large, or very large using the following tuning script.

For Cisco Prime Collaboration Assurance version 10.5 or later:

 # /opt/emms/emsam/bin/newcpcmtuning.sh

From the options displayed, choose the deployment model (excluding option 1) that you wish to upgrade to, and then select Y to proceed with upgrading or N to reselect the deployment model.

For information on installing Cisco Prime Collaboration Assurance, see Client Machine Requirements for Cisco Prime Collaboration Assurance

Downgrade the Cisco Prime Collaboration Deployment Model

Cisco Prime Collaboration does not support the downgrade of the deployment model; that is, you cannot downgrade from the Cisco Prime Collaboration large deployment model to the small deployment model.

Configure a Second NIC for Cisco Prime Collaboration Assurance

You can add a second NIC to the Cisco Prime Collaboration Assurance as follows:

- Use the vSphere Client (**Edit virtual machine settings** option) to add a second virtual network adapter to the virtual machine.
- Log in to the Cisco Prime Collaboration Assurance admin CLI to configure the IP address for the second interface.
- Configure the IP route gateways for the two interfaces (with the same CLI access).

Log in as admin user to configure the IP address for the second interface:

```
admin# configure
```

admin (config)# interface GigabitEthernet 1 (Note that the first interface is GigabitEthernet 0)

admin(config-GigabitEthernet)# ip address <ip address> <net mask> admin (config-GigabitEthernet)

 # exit

Configure the IP routes to the two different gateways:

admin (config)# ip route <network addr> <net mask> <route-specific gateway1>

admin (config)# ip route <network addr> <net mask> <route-specific gateway2> .....

Change the default route (0.0.0.0 0.0.0.0) to the appropriate gateway if needed.

Change the IP Address on the Cisco Prime Collaboration Assurance Server

The **Update System Parameters** menu in Cisco Prime Collaboration Assurance Serviceability User Interface allows you to update the system parameters. It has the provision of either entering or changing the IP address and Time Zone. System Parameters menu refers to a specific system setting. For steps to update system parameters, see Cisco Prime Collaboration Assurance Serviceability User Guide.

Step 1 Log in to CLI as admin and execute the following command:

IPAddress-Change/admin# conf t

Step 2 Execute the following configuration commands, one per line, and end each of them with "control Z".

- **IPAddress-Change/admin(config)# interface GigabitEthernet 0**
- **IPAddress-Change/admin(config-GigabitEthernet)# ip**
- **IPAddress-Change/admin(config-GigabitEthernet)# ip address 10.64.91.177 255.255.255.0**

Step 3 Enter **y** when the following message is displayed: "Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y"

Step 4 IPAddress-Change/admin(config-GigabitEthernet)# exit

Step 5 IPAddress-Change/admin(config)# exit

Step 6 IPAddress-Change/admin# wr mem

Restart VM after IP address change and execute the script **EMSAM_HOME/bin/updateJmsProps.sh**

Find the MAC Address of Cisco Prime Collaboration Assurance Servers

To find the MAC address of Cisco Prime Collaboration Assurance

Step 1 Click the About icon at the top right corner of the user interface.

Step 2 On the **About** page, click the Assurance Information link to launch the system information details for Cisco Prime Collaboration Assurance.

For all the other versions of Cisco Prime Collaboration, you can check the MAC address through the vSphere Client.

How to avoid File Not Found error during Upgrade, Restore, and Patch Installation through SFTP?

When you upgrade, restore and patch install through SFTP, copy the image to both root location and show repository output location of SFTP server to avoid **File Not Found** error.

Remove the SSL Certificate Warning

- Windows Internet Explorer—You can permanently remove the SSL certificate warning by installing the Cisco Prime Collaboration self-signed certificate.
- Mozilla Firefox—You can remove the SSL certificate warning only by adding an exception.
- Google Chrome—You can remove the SSL certificate warning by using the Manage Certificates option under HTTPS/SSL on the Settings page.

Remove the SSL Certificate Warning in Internet Explorer

Step 1 Choose **Continue to this website (not recommended)**.

Step 2 Choose **Tools** > **Internet Options**.

Step 3 In the **Internet Options** dialog box, click the **Security** tab, choose **Trusted sites**, and then click **Sites**.

Step 4 Confirm that the URL that appears in the field and matches the application URL, and then click **Add**.

Step 5 Close all dialog boxes and refresh the browser.

Step 6 Choose **Certificate Error** to the right of the address bar, and then click **View certificates**.

Step 7 In the **Certificate** dialog box, click **Install Certificate**.

Step 8 In the **Certificate Import Wizard** dialog box, click Next.

Step 9 Click the **Place all certificates in the following store** radio button, and then click **Browse**.

Step 10 In the **Select Certificate Store** dialog box, choose **Trusted Root Certification Authorities**, and then click **OK**.
Step 11 Choose **Next** > **Finish**.
Step 12 In the **Security Warning** message box, click **Yes**.
Step 13 In the **Certificate Import Wizard** message box, click **OK**.
Step 14 In the **Certificate** dialog box, click **OK**.
Step 15 Repeat Step 2 and Step 3.
Step 16 Select the URL in the **Websites** section, and then click **Remove**.

If You Have a Safe URL Implemented

Step 1 Choose **Tools** > **Internet Options** .
Step 2 In the **Internet Options** dialog box, click the **Advanced** tab .
Step 3 In the **Security** section, uncheck the **Warn about certificate address mismatch** check box.

Remove the SSL Certificate Warning in Mozilla Firefox

Step 1 Click **I Understand the Risks** >**Add Exception**.
Step 2 In the **Add Security Exception** dialog box, click **Confirm Security Exception**.