Configure System Parameters

Cisco Prime Collaboration allows you to configure system parameters for Cisco Prime Collaboration Assurance. To configure the following Cisco Prime Collaboration Assurance system parameters, navigate to **Administration > System Setup > Assurance Setup System Administration** > **Certificate Management**.

Configure SMTP Server

You can configure the SMTP server to send and receive e-mail notifications for alarms by specifying the SMTP server name and the sender AAA E-mail address on the **E-mail Setup for Alarms & Events** page (**E-mail Setup for Alarms & Events**). The value in the **Sender AAA E-mail Address** field helps you to identify the server you receive the e-mail from, in case of many servers.

SSL Certificate Authentication for Device Discovery

For Cisco Prime Collaboration Release 11.1 and earlier

In Cisco Prime Collaboration, when a device is added, the SSL certificates are exchanged for credential validation by accessing a protected resource using HTTPS. During exchange, the SSL certificate is not stored in Cisco Prime Collaboration trust-store and communication with the device fails, at a later point of time. It is recommended that you manually import the SSL certificate to Cisco Prime Collaboration trust-store to access the device.

Cisco Prime Collaboration enables you to check the authenticity of the SSL certificate during its communication with the devices or applications over HTTPS. However, this is not mandatory as you can still continue to discover the devices without authenticating the certificate.

By default, Cisco Prime Collaboration does not validate the certificates from the devices or applications it communicates.

To enable the SSL certificate authentication:

Step 1 Choose **System Administration** > **Certificate Management**.
The **Certificate Management** page is displayed.

Step 2 In the **Device Certificate Management** tab, check the **Enable SSL certificate authentication for device discovery** check box.

Step 3 Click the **Import Certificates** button.

Step 4 Restart the Cisco Prime Collaboration server for the changes in trust manager to take effect.

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

Configure Cisco Prime Collaboration Assurance Server Time Zone

To configure the Cisco Prime Collaboration Assurance server time zone:

Step 1 Log in to the Cisco Prime Collaboration Assurance server with the account that you have created during installation. By default, it is *admin*.

Step 2 Enter the following command to see the list of supported time zones:

Example:

```
cm/admin# show timezones
```

Step 3 Enter the following commands to set the time zone for the Cisco Prime Collaboration Assurance server:

Example:

```
cm/admin(config)# config t
cm/admin(config)# clock timezone US/Pacific
cm/admin(config)# exit
```

Step 4 Enter the following command to copy running-configuration to startup-configuration:

Example:

```
cm/admin# write memory
```

Step 5 Enter the following command to restart the Cisco Prime Collaboration Assurance server:

Example:

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

Step 6 Wait for 10 minutes for the server to finish the restart process and enter the following command to check if the time zone is set to the new value:

Example:

```
cm/admin# show timezone
US/Pacific
```

Note We recommended you to keep the time zone values configured in postgres database same as that of system time zone to avoid the data mismatch issues. If you change system time zone manually, then change the log_timezone and timezone parameters in `postgres.conf` file in `/opt/postgres/9.2/data` (Analytics database) and `/opt/postgres/9.2/cpcmdata` (Assurance database, including both cpcm and qovr database) to match system time zone, and then restart the system. Root access feature is mandatory to change time zone value in postgres database, hence you should raise a TAC case to obtain root access.