Configure System Parameters

This section explains the following:

Configure System Parameters

The following are the system configuration parameters for Cisco Prime Collaboration Assurance.

- SMTP Server — To configure this parameter under **Assurance Administration** > **E-mail Setup for Alarms & Events**, see Configure SMTP Server.

  For Cisco Prime Collaboration Release 11.5 and later

  SMTP Server—To configure this parameter under **Alarm & Report Administration** > **E-mail Setup for Alarms & Events**, see Configure SMTP Server.

- Call Quality Data Source Management — Cisco Prime Collaboration Assurance monitors voice-quality measurements in a VoIP network. This real-time, service-quality information is collected from Unified CMor Prime vNAM. To configure this parameter under **Assurance Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**, see Update Data Source Credentials.

  For Cisco Prime Collaboration Release 11.5 and later

  Call Quality Data Source Management — Cisco Prime Collaboration Assurance monitors voice-quality measurements in a VoIP network. This real-time, service-quality information is collected from Unified CMor Prime vNAM. To configure this parameter under **Alarm & Report Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**, see Update Data Source Credentials.

- LDAP Settings — To configure this parameter under **System Administration** > **LDAP Settings**, see Configure an LDAP Server.

- Log Management — To configure this parameter under **System Administration** > **Log Management**, see Log Levels.

- SFTP Settings — To monitor calls from Unified CM, you must configure SFTP. To configure this parameter under **Assurance Administration** > **CDR Source Settings** > **CUCM SFTP Credentials**, see Configure SFTP Settings.

  For Cisco Prime Collaboration Release 11.5 and later

SFTP Settings — To monitor calls from Unified CM, you must configure SFTP. To configure this parameter under **Alarm & Report Administration** > **CDR Source Settings** > **CUCM SFTP Credentials**, see Configure SFTP Settings.

- Cluster Device Discovery Settings - Allows Cisco Prime Collaboration Assurance to consolidate the inventory and the device registration information it collects from Unified CM. To configure this parameter under **Inventory** > **Cluster Device Discovery Schedule**, see Schedule Cluster Device Discovery.

Global System Parameters

The changes performed on these pages are applicable to all domains (Enterprise mode).

Table 1: System Parameters

Tasks	Navigation
Configure Single Sign-On.	**System Administration** > **Single Sign-On**
Add a license file.	**System Administration** > **License Management**
Configuring SMTP server.	**Alarm & Report Administration> E-mail Setup for Alarms & Events**
Configure SSL Certificate Authentication for Device Discovery.	**System Administration** > **Certificate Management**
Configure LDAP server to access user details.	**System Administration** > **LDAP Settings**
Change the log levels, the default value is “Error”.	**System Administration** > **Log Management**
Configure SFTP parameters to monitor calls from Unified CM.	**Inventory** > **Inventory Management** > **CUCM/sFTP Credentials**
Configure parameters to consolidate the inventory and the device registration information from Unified CM.	**Inventory** > **Cluster Device Discovery Schedule**
Add a dial plan.	**Alarm & Report Administration > CDR Analysis Settings > Dial Plan Configuration**
Create a call category.	**Alarm & Report Administration > CDR Analysis Settings > Call Category Configuration**
Configure parameters to poll devices.	**Alarm & Report Administration > Polling Settings**
Customize the syslog rules to monitor faults.	**Alarm & Report Administration > Event Customization > Syslog Rules**
Configure alarm notification (e-mail, syslog, or trap).	**Alarm & Report Administration> Notification Setup > Custom Notification**
Configure Voice Call Grade Settings (Good, Acceptable, Poor).	**Alarm & Report Administration > CDR Analysis Settings > Configure Voice Call Grade**

Tasks	Navigation
Configure audio phones report export parameters, such as audio phone reports (IP phone audit, move, suspect IP phones), file format, export file location, and notification e-mail.	**Reports** > **UCM/CME Phone Activity Reports** > **Export Audio Phones**
Schedule regular backups.	**System Administration** > **Backup Settings**

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.

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.