Collect Logs

This section explains the following:

Collect Logs

Cisco Prime Collaboration Assurance enables you to collect call logs to identify faults in the calls for Cisco Voice Portal (CVP), Unified Contact Center Enterprise (Unified CCE), Cisco Unified Communications Manager (Unified CM), Cisco Unity Connection (CUC), Cisco IM and Presence (Cisco IM & P), and Cisco IOS Gateways. This feature enables you to troubleshoot issues in the calls. You can use the SIP Call Flow Analyzer feature to further zoom in on the collected calls and isolate faults in the messages. It also helps you to recreate the issue. For more information on the SIP Call Flow Analyzer feature, see Analyze Call Signaling.

It helps you to:

- Reduce cost of troubleshooting issues in calls.
- Reduce time for troubleshooting issues in calls.

Prerequisites

- Ensure that you configure Debug Level for the devices using the Cisco Prime Collaboration Assurance User Interface.

The following is required/supported by this feature:

Maximum disk size required for this feature.	25 GB for small, 50 GB for medium, and very large profiles
Maximum number of devices from which log collection to be done concurrently.	100
Maximum number of log collection jobs to be run at the same time	3

Maximum size of a zipped log file that can be downloaded at one instance.	0.5 GB for small, and 1 GB for other profiles. **Note** This size is inclusive of all devices and calls. If the zipped file size exceeds the size mentioned above, the log is divided into multiple zipped files of sizes 0.5 GB for small profiles, and 1GB for other profiles.

Note

- Only logs collected from System CLI tool or another Cisco Prime Collaboration Assurance server 10.5 and later are supported.
- Time zone of the device is not collected from the System CLI tool.
- This feature also provides logs for devices which are not in Device Inventory.
- The Operator and Helpdesk users cannot collect call logs from devices and do not have access to **Device Log Collector** menu pages.

Log Collection Center/Device Log Collector

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Assurance enables you to collect call logs from the Device Log Collector available at **Diagnose** > **Device Log Collector** for the following Unified Communications (UC) components:

Device Type	Supported Release	Components or Type of Log
Cisco Unified Communications Manager (Unified CM)	9.x and later	All
IOS Gateways (TDM, CUBE (Enterprise Edition), VXML GWs)	15.1(4)M and later	Output of show logging command
Cisco Unity Connection (CUC)	9.x and later	All
Cisco IM and Presence	9.x and later	All

Devices Pane

The following information is available in the Devices pane.

- Hostname - Host name of the device
- IP Address - IP Address of the device
- Device type
- Managed in Device Inventory- Displays whether the device is in Managed state in Device Inventory or not. If the column value is No, it means that the device is not in Device Inventory and only added in Device Log Collector, or the device is not in Managed state in Device Inventory.
- Connectivity Status - Displays whether the device can be accessed with the credentials provided in Device Log Collector.

- TimeZone - Displays the device time zone.

To add or update device(s) (UC components) of Device Inventory to Device Log Collector, you can select a device, all devices of a device group and then click **Sync to Inventory Management**. The devices in the Device Log Collector and **Device Inventory** are synced in the following ways:

- Automatically: Devices from Device Inventory are synced every hour.
- Manually: When you click the **Sync to Inventory Management** button, the UC components from Device Inventory are added to the list of devices in the Device Log Collector.

Periodic sync happens every hour. Sync does not remove devices from Device Log Collector if the devices in Device Inventory are deleted. If a new device is added in Device Log Collector or any update to a device happens, then the Connectivity Status is updated after the sync.

Note

- The direction of the sync is only from Device Inventory to Device Log Collector.
- The credentials from Device Log Collector are overwritten by the credentials in Device Inventory after a sync. Thus we recommend you to keep the credentials same across Device Inventory and Device Log Collector.
- Only the devices in Managed state in Device Inventory are synced.
- If a device in Device Inventory is deleted but not deleted in Device Log Collector, you can still perform log collection in Device Log Collector,
- If the IOS gateway in Device Inventory does not have CLI credentials, it will not be synced to Device Log Collector.

Group a Device

In order to collect log from the same type of UC components on a same-time, you can create custom group of UC components and collect call logs by selecting the device group.

Predefined groups can not be added, edited, or deleted, and the devices in the groups cannot be modified too.

You can create, edit or delete user-defined groups. You can add or delete devices of the user-defined groups. You can do the following:

For Cisco Prime Collaboration Release 11.5 and later

Task	Details
Create a Group	Click **Diagnose** > **Device Log Collector** > **Group** > **Create New**.
Edit a Group	Click **Diagnose** > **Device Log Collector**, select a device or a group, and then click **Group** > **Edit Group**.
Delete a Group	Click **Diagnose** > **Device Log Collector**, select a device or a group, and then click **Group** > **Delete Group**. It takes
Add Devices to Group	Click **Diagnose** > **Device Log Collector**, select a device or a group, and then click **Group** > **Delete Group**. It takes
Delete Devices from Group	Click **Diagnose** > **Device Log Collector**, select device(s), and then click **Group** > **Add to Group**.
View Devices in Group	Select a group from the Device Group Center. The devices of that group are displayed in the Devices pane.

Other Tasks

You can perform the following tasks from the Device pane on the Device Log Collector page. Select device(s) from the Devices pane for which you want to perform the task, and then do the following as required.

Tasks	Details
Modify Credentials	Click the **Modify Credentials** button to edit the port number or credential details of device(s). You cannot modify the device type.
Modify Time zone	Click the **Modify Time Zone** button to modify the device time zone. Cisco Prime Collaboration Assurance server time zone is shown by default.

Test Connectivity of a Device

Select a device and click the **Test Connectivity** button to test if the device is accessible with credentials provided. A message is displayed to notify you about the result. The value of the column "Connectivity Status" is updated accordingly.

Troubleshoot Test Connectivity

If test connectivity fails, check the following:

- Port number
- Credentials of the device and ensure that they are same as Device Inventory.
- Ping from the Cisco Prime Collaboration Assurance Server to the device is successful.

Set the Trace Levels

This feature helps you to set the trace level for each component of the devices. You can set the trace level for the following devices:

- Cisco Unified Communications Manager
- IOS Gateway
- Customer Voice Portal
- Cisco Unity Connection
- Cisco IM and Presence

For Cisco Prime Collaboration Release 11.5 and later

Choose **Diagnose** > **Device Log Collector**.

Select the device or devices for which you want to set the trace level, and click on the **Set Trace Level to Devices** button. The Set Trace Level to Devices popup window is displayed. Select a device from the Device Type drop-down list. The components for the selected devices are listed. You can select the appropriate Trace level (No Change, Default, Warning, Information, Debug) for the components relevant to the problem you are experiencing, and click the Apply button.

Note Setting trace levels may affect network performance adversely.

Log Collection Template

The log collection template enables you to collect logs of different devices and different components together. It is mandatory to use a template to collect logs. You can create a new template or use the default template.

To create a template:

Procedure

Step 1 **For Cisco Prime Collaboration Release 11.5 and later**

Choose **Diagnose** > **Device Log Collector**, and click the **Manage Trace Template** button.

Step 2 On the Manage Trace Template page, click **Add**.

Step 3 Enter a template name and description, and select a Device Type and its components in the Component pane. You can select multiple (or all) devices and components also. For more information on the components, see Log Collection Center/Device Log Collector.

There is a default template available called Call Trace. This template has four device types - (Unified CM, Unified CCE, CVP, and IOS Gateway), and has preselected components. You cannot modify this template.

Step 4 Click **Save**. A message notifies you that the template is saved successfully. You can view the new template listed under Templates on the Manage Trace Template page.

To view the components of a particular template, select a template, and click **Summary**. To modify a template, select a template. You can modify the template name, description, and the components. To delete a template, select a template, and click **Delete**.

Note Only a Super administrator can create, edit, and delete the template. Other users can only view the template summary and use the templates for log collection.

Collect Call Logs

Log collection is on-demand.

Select a single device or devices in a group and click the **Collect Logs** button to collect logs. The Collect Logs dialog box is displayed. Fill the required information. The job name and file name are autopopulated, but you can modify it too. The time zone you select here is used to collect the logs.

Select a template from the Use Template drop-down list.

Click **Run**. A message notifies you that the job is triggered or not. The job is listed under the Log Collection Jobs pane. The Progress Status column also shows the number of devices for which the logs are downloaded out of the total number of devices selected for log collection. For example 2 of 3. You can select the job and collect the logs by clicking the **Download to local** button. If the zipped log file size is more than 0.5 GB (for small profile) or 1 GB (for medium or large profiles), it is divided into multiple zipped files.

Note Ensure that you do not modify the extension *.zip* in the file name. Sometimes the extracted file from the zipped folder may have .gz extension.

You can delete the job using the **Delete** button under the Log Collection Jobs pane.

These jobs are also listed under the Job Management page (**System Administration** > **Job Management**), however you cannot download the log file from this page.

Note If you want more information on log collection jobs, see https://<ip-address>/emsam/log/Troubleshoot/LogCollectionManagerImpl.log where IP address is the Cisco Prime Collaboration Assurance server IP address. This URL can be viewed by users with administrator role and helps you troubleshoot issues related to log collection.

Rotation functionality of Garbage Collection (GC) Log files

Note the following about the rotation functionality of GC log files:

- Cisco Prime Collaboration Assurance generates maximum three GC log files for each service.

  Example,

  `Inventory.gc.log.0,Inventory.gc.log.1,Inventory.gc.log.2`

- Cisco Prime Collaboration Assurance appends ".current" extension to the name of the file in which it records the logs now.

  Usually, the first file generated is `Inventory.gc.log.0` and Assurance renames it as `Inventory.gc.log.0.current`.

- For small, and medium deployment model, the size of each GC file is 256 MB. For large, very large, and super large deployment models, the size of each GC file is 512 MB.

- Once the `Inventory.gc.log.0.current` reaches the maximum size, Cisco Prime Collaboration Assurance generates the next GC file, `Inventory.gc.log.1`.

  It then appends the file name with the ".current" extension, `Inventory.gc.log.1.current`. `Inventory.gc.log.0` remains as it is.

- Cisco Prime Collaboration Assurance does not delete old GC files. Once files reaches maximum rotation number ie, `Inventory.gc.log.2`, the system overwrites and records the next set of logs in `Inventory.gc.log.0`. This process of rotation continues.

Note This is the default behaviour of GC log rotation.